

Computing Integral Points on $X_{\text{ns}}^+(p)$

Aurélien Bajolet, Yuri Bilu*

December 5, 2012

Contents

1	Introduction	1
2	Modular Curves, Fundamental Domains, q-Parameters	3
3	Integral Points and Baker's Method	6
4	Siegel Functions	8
5	General Modular Units	13
6	Cusp Points and Units on $X_{\text{ns}}^+(p)$	16
7	The Principal Relation	21
8	Baker's Method on $X_{\text{ns}}^+(p)$	23
9	Reduction of Baker's Bound	27
10	Final enumeration	28

1 Introduction

In his celebrated work of 1978 Mazur [25] completely described possible rational points on the modular curves $X_0(p)$, where p is a prime number. In particular, he showed that the set $X_0(p)(\mathbb{Q})$ consists only of the cusps if $p > 163$, and of the cusps and the CM-points if $37 < p \leq 163$.

The curve $X_0(p)$ associated to the Borel subgroup of $\text{GL}_2(\mathbb{F}_p)$. It is natural to ask the same question on the modular curves associated to two other important maximal subgroups of $\text{GL}_2(\mathbb{F}_p)$, the normalizers of a split or a non-split Cartan subgroups (see [30, Appendix A.5] or [5, Section 2] for the definitions). We shall denote these curves $X_{\text{sp}}^+(p)$ and $X_{\text{ns}}^+(p)$, respectively. This problem is not only interesting by itself, but is also motivated by applications; for instance, Serre's uniformity problem about Galois representations [12] would be solved if one show that for large p the sets $X_{\text{sp}}^+(p)(\mathbb{Q})$ and $X_{\text{ns}}^+(p)(\mathbb{Q})$ consist only of the cusps and the CM-points (points corresponding to elliptic curves with complex multiplication). For the convenience of the reader, we reproduce the full list of the 13 rational CM j -invariants in Table 1.

Rational points on the curves $X_{\text{sp}}^+(p)$ were determined recently [13, 14] for all $p \neq 13$; in particular, it is shown in [14] that for $p \geq 17$ the set $X_{\text{sp}}^+(p)(\mathbb{Q})$ consists only of the cusps and the CM-points.

Unfortunately, the methods of [13, 14] completely fail for the curve $X_{\text{ns}}^+(p)$. To the best of our knowledge, the set $X_{\text{ns}}^+(p)(\mathbb{Q})$ is not known for every prime $p \geq 13$.

More is known about *integral* points on the curves $X_{\text{ns}}^+(p)$, that is, points $P \in X_{\text{ns}}^+(p)(\mathbb{Q})$ such that $j(P) \in \mathbb{Z}$, where j is the modular invariant. Kenku [19] determined the integral points on the curve $X_{\text{ns}}^+(7)$; in fact, he found the 7-integral points, that is, such that the denominator of $j(P)$ is a power of 7. He used in an essential way the fact that the curve is of genus 0.

More recently, Schoof and Tzanakis [29] determined the integral points on $X_{\text{ns}}^+(11)$, using the fact that this curve is of genus 1. They showed that the only integral points on this curve are the CM-points. See also [15].

*Supported by the Agence Nationale de la Recherche project "Hamot" (ANR 2010 BLAN-0115-01) and by the ALGANT scholarship program.

$\frac{df^2}{j} \mid$	-3	$-3 \cdot 2^2$	$-3 \cdot 3^3$	-4	$-4 \cdot 2^2$	-7	$-7 \cdot 2^2$	-8
	0	$2^4 3^3 5^3$	$-2^{15} 3 \cdot 5^3$	$2^6 3^3$	$2^3 3^3 11^3$	$-3^3 5^3$	$3^3 5^3 17^3$	$2^6 5^3$
$\frac{df^2}{j} \mid$	-11	-19	-43	-67	-163			
	-2^{15}	$-2^{15} 3^3$	$-2^{18} 3^3 5^3$	$-2^{15} 3^3 5^3 11^3$	$-2^{18} 3^3 5^3 23^3 29^3$			

Table 1: Rational CM j -invariants
together with the discriminant of the CM order

We may also mention that integral points on the curve $X_{\text{ns}}^+(N)$ of certain composite levels N were determined much earlier by Heegner and Siegel [17, 33] in the context of the Class Number 1 problem; see [30, Appendix A.5] for more details. More recently, composite levels were examined by Baran [4, 5]. Non of these methods seems to extend to higher prime levels either.

In [1] Bajolet and Sha, using Baker’s method, obtained a fully explicit upper bound for the size of an integral point P on $X_{\text{ns}}^+(p)$ for an arbitrary prime $p \geq 7$. They showed that in general

$$\log |j(P)| < 41993 \cdot 13^p \cdot p^{2p+7.5} (\log p)^2, \quad (1)$$

and this bound can be substantially refined if $p-1$ is divisible by a small odd prime or by 8. Sha [31, 32] extended the result of [1] to S -integral points on rather general modular curves over arbitrary number fields, giving an explicit version of the “effective Siegel’s theorem for modular curves” [6, 11].

Using bound (1), one can, in principle, enumerate all integral points on $X_{\text{ns}}^+(p)$. However, this bound is too huge to perform this enumeration in reasonable time.

It turns out that the huge bound can be reduced using the numerical Diophantine approximation techniques, which go back to the work of Baker and Davenport [3]. The idea of Baker and Davenport was elaborated in [7, 8, 9, 10, 16, 27, 34] in the context of the Diophantine equations of Thue and of related types, providing practical methods for solving these equations.

In the present article we adapt these techniques to modular curves and develop an algorithm for finding integral points on the modular curve $X_{\text{ns}}^+(p)$, where $p \geq 7$ is an arbitrary prime number. Having implemented our algorithm, we prove the following.

Theorem 1.1 *Let p be a prime number, $11 \leq p \leq 67$, and let $P \in X_{\text{ns}}^+(p)(\mathbb{Q})$ be such that $j(P) \in \mathbb{Z}$. Then P is a CM point (that is, $j(P)$ is one of the 13 numbers displayed in the second line of Table 1).*

One may conjecture that for any prime $p \geq 11$ the only integral points on $X_{\text{ns}}^+(p)$ are the CM-points.

1.1 Plan of the article

In Section 2 we recall basic definitions about modular curves. In particular, we remind the notions of the *nearest cusp* and the *q -parameter* at a given cusp, a basic tools in the calculus on modular curves.

In Section 3 we give a general informal overview on how Baker’s method applies to modular curves, highlighting both theoretical and numerical aspects.

In Sections 4 and 5 we revise the theory of modular units, an indispensable tool in the Diophantine analysis of modular curves. In Section 6 we apply this general theory in the special case of the curve $X_{\text{ns}}^+(p)$, constructing especially “economical” units on this curve.

In Section 7 we evaluate the unit constructed in Section 6 at an integral point P , and express the value as multiplicative combination of certain algebraic numbers: $U(P) = \eta_0^{b_0} \eta_1^{b_1} \cdots \eta_r^{b_r}$. We then express the exponents b_k in terms of the q -parameter of P . These expression, while pretty trivial, will play fundamental role in the remaining part of the article.

In Section 8 we use Baker’s method to obtain a huge explicit bound for $B = \max_k |b_k|$. We follow [1] with the modifications stemming from our present needs. In Section 9 we show how this bound can be drastically reduced in practical situations. In the final section we show how to check which values of b_k below the reduced bound indeed correspond to an integral point.

1.2 Notation and Conventions

Modular functions Throughout the article, the letter j may have four different meaning, sometimes in the same equation, like in (4) and (6): the modular invariant $j(\tau)$ on the Poincaré upper halfplane \mathcal{H} ; the modular invariant $j(E)$ of an elliptic curve E ; the “modular invariant” rational function on a modular curve; the sum of the familiar series $j(q) = q^{-1} + 744 + 196884q + \dots$. It should be always clear from the context which meaning of j is used. A similar convention applies to other modular functions as well.

The $O_1(\cdot)$ notation We shall use the notation $O_1(\cdot)$, which is a quantitative analogue of the familiar $O(\cdot)$. Precisely, $A = O_1(B)$ means that $|A| \leq B$.

Absolute Values and Heights Absolute values on number fields are normalized to extend standard absolute values on \mathbb{Q} : $|p|_v = p^{-1}$ if $v \mid p < \infty$ and $|2013|_v = 2013$ if $v \mid \infty$. We denote by $h(\cdot)$ the usual *absolute logarithmic height*: if $\alpha \in \mathbb{Q}$ then

$$h(\alpha) = [K : \mathbb{Q}]^{-1} \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log^+ |\alpha|_v, \quad \log^+ = \max\{\log, 0\}.$$

where K is a number field containing α . If $\alpha \in \mathcal{O}_K$ then

$$h(\alpha) = [K : \mathbb{Q}]^{-1} \sum_{\sigma: K \hookrightarrow \mathbb{C}} \log^+ |\alpha^\sigma|,$$

the sum being over the complex embeddings of K .

2 Modular Curves, Fundamental Domains, q -Parameters

Let N be a positive integer. The modular curve $X(N)$ has a geometrically irreducible model over the cyclotomic field $\mathbb{Q}(\zeta_N)$, and the Galois group $\text{Gal}(\mathbb{Q}(\zeta_N)(X(N))/\mathbb{Q}(j))$ is canonically isomorphic to $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$, with $\text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ being the group $\text{Gal}(\mathbb{Q}(\zeta_N)(X(N))/\mathbb{Q}(\zeta_N, j))$, see [22, Chapter 6]. We write the Galois action of $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the field $\mathbb{Q}(\zeta_N)(X(N))$ exponentially. In the following proposition we collect the properties of this action.

Proposition 2.1 1. For $f \in \mathbb{Q}(\zeta_N)(X(N))$ and $\sigma \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ we have

$$f^\sigma = f \circ \tilde{\sigma},$$

where on the right we view f as a $\Gamma(N)$ -automorphic function on the extended Poincaré plane $\tilde{\mathcal{H}}$, and $\tilde{\sigma}$ is a lifting of σ to $\Gamma(1) = \text{SL}_2(\mathbb{Z})$. Clearly, the result is independent of the choice of the lifting.

2. For $\sigma \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ we have

$$\zeta_N^\sigma = \zeta_N^{\det \sigma}. \tag{2}$$

3. Recall that $f \in \mathbb{Q}(\zeta_N)(X(N))$ has the “ q -expansion”

$$f = \sum_{k=k_0}^{\infty} a_k q^{k/N} \in \mathbb{Q}(\zeta_N)((q)).$$

Then for $\sigma = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ the q -expansion of f^σ is

$$f^\sigma = \sum_{k=k_0}^{\infty} a_k^\sigma q^{k/N}.$$

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ containing $-I$. We denote by X_G the associated modular curve. It corresponds to the G -invariant subfield of the field $\mathbb{Q}(\zeta_N)(X(N))$. The constant subfield of this field is $\mathbb{Q}(\zeta_N)^{\det G}$, where $\det : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \rightarrow (\mathbb{Z}/N\mathbb{Z})^\times$ is the determinant, and we identify $(\mathbb{Z}/N\mathbb{Z})^\times$ with the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. In particular, if $\det G = (\mathbb{Z}/N\mathbb{Z})^\times$ then the constant subfield is \mathbb{Q} and the corresponding modular curve X_G is defined (that is, has a geometrically irreducible model) over \mathbb{Q} .

For a subgroup H of $(\mathbb{Z}/N\mathbb{Z})^\times$ put

$$G_H = \{g \in G : \det g \in H\}. \quad (3)$$

In particular, $G_{(\mathbb{Z}/N\mathbb{Z})^\times} = G$ and $G_1 = G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. If H is contained in $\det G$, then the subfield of $\mathbb{Q}(\zeta_N(X(N)))$ stabilized by G_H is $K(X_G)$, where $K = \mathbb{Q}(\zeta_N)^H$.

Remark 2.2 Let M_N be the subset of the abelian group $(\mathbb{Z}/N\mathbb{Z})^2$ consisting of the elements of exact order N . Then the set of cusps of the modular curve X_G stays in natural one-to-one correspondence with the set $G_1 \backslash M_N$ of orbits of the natural (left) action of G_1 on M_N [11, Lemma 2.3]. Formally, we do not need this property of cusps in the present article, but it provides a nice “visual” presentation of the cusps; we shall use it in Section 6.

The cusps are defined over the cyclotomic field $\mathbb{Q}(\zeta_N)$. Identifying the groups $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ and $(\mathbb{Z}/N\mathbb{Z})^\times$, the natural left action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on the set $G_1 \backslash M_N$ coincides with the Galois action on the cusps. Hence, if H is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ then the set of H -orbits of cusps stands in a one-to-one correspondence with (left) G_H -orbits on M_N .

2.1 Optimal System of Representatives

Let Γ be the subgroup of $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ obtained by lifting G_1 . Then the set of complex points $X_G(\mathbb{C})$ is analytically isomorphic to $\Gamma \backslash \bar{\mathcal{H}}$, where $\bar{\mathcal{H}} = \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}$ is the extended Poincaré plane.

Let Σ be a system of representatives of the right cosets $\Gamma \backslash \Gamma(1)$. We say that Σ is an *optimal* system of representatives if it has the following property: given $\sigma_1, \sigma_2 \in \Sigma$ such that $\sigma_1(i\infty)$ and $\sigma_2(i\infty)$ are Γ -equivalent, we have $\sigma_1(i\infty) = \sigma_2(i\infty)$. An optimal system of representatives always exists. Indeed, start from any Σ . The Γ -equivalence of $\sigma_1(i\infty)$ and $\sigma_2(i\infty)$ defines an equivalence relation on Σ . Fix an equivalence class $\sigma_1, \dots, \sigma_m$. Then there exist $\gamma_2, \dots, \gamma_m \in \Gamma$ such that $\sigma_1(i\infty) = \gamma_k \circ \sigma_k(i\infty)$ for $k = 2, \dots, m$. Replacing $\sigma_2, \dots, \sigma_m$ by $\gamma_2 \circ \sigma_2, \dots, \gamma_m \circ \sigma_m$, and doing a similar operation for every other equivalence class, we obtain an optimal system of representatives.

Moreover, the argument of the previous paragraph shows the following. Let Σ' be a subset of $\Gamma(1)$ with the property that for any two elements $\sigma'_1, \sigma'_2 \in \Sigma'$ the points $\sigma'_1(i\infty)$ and $\sigma'_2(i\infty)$ are *not* Γ -equivalent. Then Σ' can be completed to an optimal system of representatives of $\Gamma \backslash \Gamma(1)$.

We fix, once and for all, an optimal system of representatives Σ . The function $\tau \mapsto q(\tau) = e^{2\pi i \tau}$ is an analytic function on \mathcal{H} , which vanishes at $i\infty$; it will be called the *q-parameter*. For every cusp c of our curve X_G we define the *q-parameter at c* as follows. Let $\sigma \in \Sigma$ be such that $\sigma(i\infty)$ represents c . Then the *q-parameter at c* is defined by $q_c = q \circ \sigma^{-1}$. Since Σ is optimal, q_c depends only on Σ , but not on the particular choice of σ . The function q_c is analytic on \mathcal{H} and vanishes at $\sigma(i\infty)$.

2.2 The Fundamental Domain and the q-Parameters

We denote by D the familiar fundamental domain of the modular group $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$: the hyperbolic triangular with vertices $e^{i\pi/3}, e^{2i\pi/3}, i\infty$, and with the geodesics $(i, e^{2i\pi/3}]$ and $[e^{2i\pi/3}, i\infty]$ excluded. Then the set

$$\Delta = \bigcup_{\sigma \in \Sigma} \sigma D$$

is a fundamental domain for Γ . This means that there is a bijection between the set Δ and the set $Y_G(p)(\mathbb{C})$ of non-cuspidal complex points of X_G . Thus, to every non-cuspidal $P \in X_G(\mathbb{C})$ we uniquely associate $\tau = \tau(P) \in \Delta$.

Further, there is a natural projection $\Delta \rightarrow D$, coinciding with σ^{-1} on every σD . The image of $\tau(P)$ under this projection will be called $\tau_0(P)$. For a non-cuspidal complex point P we have

$$\begin{aligned} |\tau_0(P)| &\geq 1, & \text{Im} \tau_0(P) &\geq \sqrt{3}/2 \\ j(P) &= j(\tau(P)) = j(\tau_0(P)) \end{aligned} \quad (4)$$

For every cusp c we define the Ω_c in $X_G(\mathbb{C})$ by

$$\Omega_c = \text{the image of } \left(\bigcup_{\sigma(i\infty)=c} \sigma D \right) \cup \{c\}, \quad (5)$$

the union being over all $\sigma \in \Sigma$ representing the cusp c . The sets Ω_c are pairwise disjoint and cover $X_G(\mathbb{C})$:

$$\bigcup_c \Omega_c = X_G(\mathbb{C}), \quad \Omega_c \cap \Omega_{c'} = \emptyset \quad (c \neq c').$$

If $P \in X_G(\mathbb{C})$ belongs to Ω_c , we call c the *nearest cusp* to P .

The q -parameter q_c defines a holomorphic function on an open neighborhood of Ω_c ; this function is denoted by q_c . For $P \in \Omega_c$ we have $q_c(P) = e^{2\pi i \tau_0(P)}$ and

$$j(P) = j(q_c(P)) \quad (6)$$

Since $\text{Im} \tau_0(P) \geq \sqrt{3}/2$ for $P \in \Omega_c$, we have

$$|q_c(P)| \leq e^{-\pi\sqrt{3}} < 0.0044. \quad (7)$$

Denote by e_c the ramification index at c of the natural morphism $X_G \rightarrow X(1)$. Then q_c^{1/e_c} can be viewed as a “local parameter” at c . This means the following: if $u \in \mathbb{C}(X_G)$ is a \mathbb{C} -rational function on X_G , then in a neighborhood of c we have

$$\log |u(P)| = \frac{\text{Ord}_c u}{e_c} \log |q_c(P)| + O(1). \quad (8)$$

The following property will be routinely used.

Proposition 2.3 *For a non-cusp point $P \in X_G(\mathbb{C})$ the following two conditions are equivalent.*

1. $j(P) \in \mathbb{R}$;
2. $\text{Re}(\tau_0(P)) \in \{0, 1/2\}$ or $|\tau_0(P)| = 1$.

More precisely:

$$\begin{aligned} j(P) \in [1728, +\infty) &\iff \text{Re}(\tau_0(P)) = 0 &\iff q_c(P) > 0, \\ j(P) \in [-\infty, 0) &\iff \text{Re}(\tau_0(P)) = 1/2 &\iff q_c(P) < 0, \\ j(P) \in [0; 1728] &\iff |\tau_0(P)| = 1, \end{aligned}$$

where c is the nearest cusp to P .

We shall also need an approximate formula for the the j -invariant. Write the familiar expansion as¹

$$j(q) = q^{-1} + c_0 + c_1 q + c_2 q^2 + \dots,$$

with $c_0 = 744$, $c_1 = 196884$ etc. For a positive integer N write

$$j_N(q) = q^{-1} + \sum_{n=0}^N c_n q^n.$$

¹The coefficients c_n cannot be confused with the cusps.

Lemma 2.4 *For $P \in \Omega_c$ we have*

$$j(P) = j_N(q_c(P)) + R_N, \quad |R_N| \leq j(e^{-\pi\sqrt{3}}) - j_N(e^{-\pi\sqrt{3}}) \quad (9)$$

for any positive integer N .

Proof Since j is $\Gamma(1)$ -invariant, we may assume that c is the cusp at infinity and $q_c(P) = q(P)$. Since the coefficients c_n are known to be positive and $|q(P)| \leq e^{-\pi\sqrt{3}}$, we have

$$|j(P) - j_N(q_c(P))| \leq \sum_{n=N+1}^{\infty} c_n |q(P)|^n \leq \sum_{n=N+1}^{\infty} c_n |e^{-\pi\sqrt{3}}|^n = j(e^{-\pi\sqrt{3}}) - j_N(e^{-\pi\sqrt{3}}),$$

proving (9). □

3 Integral Points and Baker's Method

In this section we give a general overview of Baker's method applied to modular curves. For more details, see [6].

Let N and G be as in Section 2, let K be a number field containing $\mathbb{Q}(\zeta_N)^{\det G}$ and \mathcal{O}_K the ring of integers of K . We define the set of integral points

$$X_G(\mathcal{O}_K) = \{P \in X_G(K) : j(P) \in \mathcal{O}_K\}.$$

We want to bound the height $h(j(P))$ for $P \in X_G(\mathcal{O}_K)$. We show how to do this under the assumption

$$\nu_{\infty}(G) \geq 3, \quad (10)$$

where $\nu_{\infty}(G)$ denotes the number of cusps of X_G .

A *modular unit* is a rational function (defined over \bar{K}) on X_G with no zeros and no poles outside the cusps. Equivalently, $u \in \bar{K}(X_G)$ is a modular unit if both u and u^{-1} are integral over the ring $\mathbb{Q}[j]$. Principal divisors of modular units form a subgroup in the group of degree 0 divisors supported on the cusps. The latter is a free abelian group of rank $\nu_{\infty}(G) - 1$, so the group of principal divisors of modular units must be of rank not exceeding $\nu_{\infty}(G) - 1$. It is of fundamental importance for us that it is of the maximal possible rank; this is sometimes called the “Manin-Drinfeld theorem”.

Theorem 3.1 *The principal divisors of modular units form a free abelian group of rank $\nu_{\infty}(G) - 1$.*

See [23, Chapter 4, Theorem 2.1]. Here is an immediate consequence.

Corollary 3.2 *Assume that $\nu_{\infty}(G) \geq 3$. Then for any cusp c there exists a non-constant modular unit u such that $u(c) = 1$.*

If $j(P) \in \mathcal{O}_K$ then $h(j(P)) = [K : \mathbb{Q}]^{-1} \sum_{\sigma: K \hookrightarrow \mathbb{C}} \log^+ |j(P)^{\sigma}|$, the sum being over the complex embeddings of K . For some embedding σ we have $h(j(P)) \leq \log |j(P)^{\sigma}|$. We fix this embedding from now on and view K as a subfield of \mathbb{C} . Thus, we have to bound $|j(P)|$ from above.

The point P belongs to one of the sets Ω_c , defined in (5), and the corresponding c is the “nearest cusp” to P . Now, since $\nu_{\infty}(G) \geq 3$, we may use Corollary 3.2 and find a non-constant modular unit u with $u(c) = 1$. The rational function u is defined over the number field $K(\zeta_N)$.

If $u(P) = 1$ then it is easy to bound P as one of the zeros of the rational function $u - 1$. From now on we assume that $u(P) \neq 1$. Since $u(c) = 1$, we have

$$u(P) = 1 + O(|q_c(P)|^{1/\epsilon_c}).$$

(Here and below in this section, the constant implied by the $O(\cdot)$ -notation, as well as by the Vinogradov notation “ \ll ” and “ \gg ”, may depend on N and K , but not on P .) Thus, $u(P)$ is a complex algebraic number, distinct from 1 but “close” to 1 if $q_c(P)$ is small.

Since both u and u^{-1} are integral over $\mathbb{Q}[j]$, that there exist non-zero $A, B \in \mathbb{Z}$, which can be easily determined explicitly, such that Au and Bu^{-1} are integral over $\mathbb{Z}[j]$. Since $j(P) \in \mathcal{O}_K$, both $Au(P)$ and $Bu(P)^{-1}$ belong to $\mathcal{O}_{K(\zeta_N)}$. It follows that there are only finitely many possibilities for the principal ideal $(u(P))$ (viewed as a fractional ideal in the field $K(\zeta_N)$). In other words, we have $u(P) = \eta_0 \eta$, where η_0 belongs to a finite subset of K (that can be explicitly determined), and η is a Dirichlet unit of K . Fixing a base η_1, \dots, η_r of the group of Dirichlet units of $K(\zeta_N)$, we obtain $u(P) = \eta_0 \eta_1^{b_1} \cdots \eta_r^{b_r}$, where b_1, \dots, b_r are rational integers depending of P . We obtain the inequality

$$\left| \eta_0 \eta_1^{b_1} \cdots \eta_r^{b_r} - 1 \right| \ll q_c(P)^{1/e_c}. \quad (11)$$

It is easy to show that $B \ll h(\eta)$, see [6, bottom of page 77]. It follows that $B \ll h(u(P)) + 1$. On the other hand, the general property of quasi-equivalence of heights on an algebraic curve implies that $h(u(P)) \ll h(j(P)) + 1$. It follows that

$$B \ll h(j(P)) \leq \log |j(P)| = \log |q_c(P)^{-1}| + O(1). \quad (12)$$

On the other hand, one can bound the left-hand side of (11) from below using the so-called *Baker’s inequality*. We state it in a full detail in Section 8. Here we just remark that Baker’s inequality implies that either the left-hand side of (11) is 0 (in which case $u(P) = \beta_c$ and $h(j(P))$ is bounded), or it is bounded from below by $\exp(-\kappa \log B)$, where $B = \max\{|b_1|, \dots, |b_r|, 3\}$ and κ is a positive effective constant depending on $\eta_0, \eta_1, \dots, \eta_r$ but independent of B . Combining this with (11), we obtain $\log |q_c(P)^{-1}| \ll \log B$. Together with (12) this bounds $|q_c(P)|$ from below, which implies a bound for $|j(P)|$ from above.

In a similar fashion one can study S -integral points on X_G : the new ingredients to be added are the p -adic version of Baker’s inequality, due to Yu [35], and the p -adic analogue of the notion of the “nearest cusp”, see [12, Section 3]. To make all this explicit, one needs to construct modular units explicitly. The standard tool for this are *Siegel functions*, see Section 4 below. One also needs explicit version for various statements above like the quasi-equivalence of heights, etc. All this is a part of a forthcoming Ph.D. thesis of Sha [31, 32].

In the present work, we are interested in a somewhat different task: not just bound the heights of integral points, but determine them completely. We restrict ourselves to the case $K = \mathbb{Q}$ and $N = p$ a prime number. In this case the most interesting class of modular curves for which integral points are unknown is $X_{\text{ns}}^+(p)$, when the group G is the normalizer of a non-split Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$.

The principal point here is that bounding the height of integral points, even explicitly in all parameters, is not sufficient for the actual calculation of the points. The problem is that the bounds obtained by Baker’s method are very high and not suitable for computational purposes.

Fortunately, one can reduce Baker’s bound using the technique of numerical Diophantine approximations. This reduction is described in detail in [7, 9, 16] in the context of the Diophantine equation of Thue. Recall that this is the equation of the form $f(x, y) = A$, where the $f(x, y) \in \mathbb{Z}[x, y]$ is a \mathbb{Q} -irreducible form of degree $n \geq 3$, and A is a non-zero integer. In [8] the method was extended to the superelliptic Diophantine equations. Here we adapt this reduction method to the modular curves.

Several observations are to be made.

1. Usually, to perform the computations, one should know explicitly the algebraic data of the number field(s) involved (in the case of Thue equation, this is the field generated over \mathbb{Q} by a root of $f(1, y)$). By the algebraic data we mean here the unit group (with explicit generators), the class group (again, for every class one should have an explicit ideal representing this class), and so on. Fortunately, in the special case of the curve $X_{\text{ns}}^+(p)$ these tasks are radically simplified. First, the field we are going to deal with is the real cyclotomic field $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ (or its subfield, see below) for which the unit group (or at least a full-rank subgroup of the latter,

which is sufficient, see below) are given explicitly by the *circular units*. Second, the only ideal we are going to deal with is the one above p , which is principal and has an obvious explicit generator $(\zeta_p - \bar{\zeta}_p)^2$. This was already used in [10] for solving Thue equations $\Phi_n(x, y) = p$, where $\Phi_n(1, y)$ is the n -th real cyclotomic polynomial, and p is a primer divisor of n .

2. To make the calculations more efficient, it is useful to replace the field $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ by a smaller subfield, whenever possible. This was suggested in [9] and was very efficiently exploited in [10].
3. Also, it is not necessary to have the full unit group; a full-rank subgroup would suffice, as explained in [16]. This was used in [10] as well. In the present work we use only full unit groups, but one should keep this opportunity in mind for further applications.
4. Adapting numerical methods developed for Thue equations to modular curves is not straightforward. In the Thue case one has formulas with very strong error estimates, typically $O(|x|^{-n})$, where n is the degree of the equation; see, for instance [7, Proposition 2.4.1]. This is quite good even for small solutions x . However, for modular curves of level p we have, typically, errors $O(|j(P)|^{-1/p})$. For small solutions this error can be too large to deal with, and we have to use high order asymptotic expansions for the modular functions involved, which makes the things more complicated. See Subsection 10.2.

4 Siegel Functions

In this section we recall the principal facts about Klein forms and Siegel functions. For more details the reader can consult [21, Section 2.1] and [20].

4.1 Klein Forms and Siegel Functions

Let $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2$ be such that $\mathbf{a} \notin \mathbb{Z}^2$. We denote by $\mathfrak{k}_{\mathbf{a}}(\tau)$ the Klein form associated to \mathbf{a} , which is a holomorphic function on the Poincaré plane \mathcal{H} . We collect some properties Klein forms in the proposition below.

Proposition 4.1 1. *The Klein forms do not vanish on \mathcal{H} .*

2. *The Klein forms well behave under the action of $\Gamma(1)$: for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ we have*

$$\mathfrak{k}_{\mathbf{a}} \circ \gamma(\tau) = (c\tau + d)^{-1} \mathfrak{k}_{\mathbf{a}\gamma}(\tau),$$

where $\gamma(\tau) = \frac{a\tau+b}{c\tau+d}$. In particular, with $\gamma = -I$ this gives

$$\mathfrak{k}_{-\mathbf{a}} = -\mathfrak{k}_{\mathbf{a}}. \tag{13}$$

3. *For $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ and $\mathbf{b} = (b_1, b_2) \in \mathbb{Z}^2$ we have*

$$\mathfrak{k}_{\mathbf{a}+\mathbf{b}} = \varepsilon(\mathbf{a}, \mathbf{b}) \mathfrak{k}_{\mathbf{a}}, \quad \varepsilon(\mathbf{a}, \mathbf{b}) = (-1)^{b_1 b_2 + b_1 + b_2} e^{\pi i(a_1 b_2 - a_2 b_1)}.$$

Notice that $\varepsilon(\mathbf{a}, \mathbf{b})^{2N} = 1$, where N is a denominator of \mathbf{a} (a common denominator of a_1 and a_2).

4. *Let N be a denominator of \mathbf{a} . Then $\mathfrak{k}_{\mathbf{a}}$ is “nearly” $\Gamma(N)$ -automorphic of weight -1 . Precisely, for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(N)$ we have*

$$\mathfrak{k}_{\mathbf{a}} \circ \gamma(\tau) = \varepsilon'(\mathbf{a}, \gamma)(c\tau + d)^{-1} \mathfrak{k}_{\mathbf{a}}(\tau), \quad \varepsilon'(\mathbf{a}, \gamma)^{2N} = 1.$$

The following result is a consequence of the properties above.

Proposition 4.2 *Let N be a denominator of \mathbf{a} . Then $\mathfrak{k}_{\mathbf{a}}^{2N}$ depends only on the residue class of \mathbf{a} modulo \mathbb{Z}^2 , and is $\Gamma(N)$ -automorphic of weight $-2N$.*

Further, for $\mathbf{a} = (a_1, a_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ we define the *Siegel function* $g_{\mathbf{a}}(\tau)$ by

$$g_{\mathbf{a}}(\tau) = \mathfrak{k}_{\mathbf{a}}(\tau) \eta(\tau)^2,$$

where $\eta(\tau)$ is the Dedekind η -function.

As usual, write $q = q(\tau) = e^{2\pi i \tau}$. For a rational number a we define $q^a = e^{2\pi i a \tau}$. Then the Siegel function $g_{\mathbf{a}}$ has the following infinite product presentation [21, page 29]:

$$g_{\mathbf{a}}(\tau) = -q^{B_2(a_1)/2} e^{\pi i a_2(a_1-1)} \prod_{n=0}^{\infty} (1 - q^{n+a_1} e^{2\pi i a_2}) (1 - q^{n+1-a_1} e^{-2\pi i a_2}), \quad (14)$$

where $B_2(T)$ is the second Bernoulli polynomial. Together with item 3 of Proposition 4.1 this has the following consequence.

Proposition 4.3 *We have $\text{Ord}_q g_{\mathbf{a}} = \ell_{\mathbf{a}}$, where $\ell_{\mathbf{a}} = B_2(a_1 - \lfloor a_1 \rfloor)/2$.*

Here the q -order Ord_q is defined by $\lim_{q \rightarrow 0} q^{\text{Ord}_q g_{\mathbf{a}}} g_{\mathbf{a}}(q) \neq 0, \infty$.

Since $\eta(\tau)^{24} = \Delta(\tau)$ is $\Gamma(1)$ -automorphic of weight 12, Proposition 4.2 implies the following.

Theorem 4.4 *In the set-up of Proposition 4.2, the function $g_{\mathbf{a}}^{12N}$ depends only on the residue class of \mathbf{a} modulo \mathbb{Z}^2 , and is $\Gamma(N)$ -automorphic of weight 0.*

It follows, in particular, that Siegel functions $g_{\mathbf{a}}$ are algebraic over the field $\mathbb{C}(j)$ (because so are $\Gamma(N)$ -automorphic functions). In addition to this, $g_{\mathbf{a}}$ is holomorphic and does not vanish on the Poincaré plane \mathcal{H} (because so are the Klein forms and the Dedekind η). It follows that both $g_{\mathbf{a}}$ and $g_{\mathbf{a}}^{-1}$ must be integral over the ring $\mathbb{C}[j]$. Actually, a stronger assertion holds (see, for instance, Proposition 2.2 from [13]).

Proposition 4.5 *Let N be the smallest denominator of \mathbf{a} and ζ_N a primitive N -th root of unity. Then both $g_{\mathbf{a}}$ and $(1 - \zeta_N) g_{\mathbf{a}}^{-1}$ are integral over $\mathbb{Z}[j]$.*

4.2 Simplest Modular Units

Now let us fix a positive integer N . By Theorem 4.4, for $\mathbf{a} \in N^{-1}\mathbb{Z}^2 \setminus \mathbb{Z}^2$ the function $g_{\mathbf{a}}^{12N}$ defines a \mathbb{C} -rational function on the modular curve $X(N)$, to be denoted by $u_{\mathbf{a}}$. Moreover, $u_{\mathbf{a}}$ is well-defined when \mathbf{a} is a non-zero element of the abelian group $(N^{-1}\mathbb{Z}/\mathbb{Z})^2$, which will be assumed until the end of the subsection. Identity (13) implies that $u_{\mathbf{a}} = u_{-\mathbf{a}}$.

The infinite product (14) implies that the q -expansion of $u_{\mathbf{a}}$ has coefficients in the cyclotomic field $\mathbb{Q}(\zeta_N)$. It follows that $u_{\mathbf{a}} \in \mathbb{Q}(\zeta_N)(X(N))$. Moreover, the Galois action of the group $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the field $\mathbb{Q}(\zeta_N)(X(N))$ (see Section 2) is compatible with the natural right action of on the set $(N^{-1}\mathbb{Z}/\mathbb{Z})^2$ in the following sense: for a non-zero $\mathbf{a} \in (N^{-1}\mathbb{Z}/\mathbb{Z})^2$ and $\sigma \in \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ we have

$$u_{\mathbf{a}\sigma} = u_{\mathbf{a}}^{\sigma}. \quad (15)$$

See [12, Section 4.2] for more details.

The functions $u_{\mathbf{a}}$ give simplest explicit examples of the *modular units*, already mentioned in Section 3: they have no zeros and no poles outside the cusps. It follows that their principal divisors generate a free abelian subgroup of rank at most $\nu_{\infty}(N) - 1$, where $\nu_{\infty}(N)$ is the number of cusps of $X(N)$. It turns out that this rank is maximal possible, which provides an explicit form of the “Manin-Drinfeld theorem” (Theorem 3.1):

Theorem 4.6 *The principal divisors $(u_{\mathbf{a}})$ generate a free abelian group of rank $\nu_{\infty}(N) - 1$.*

For the proof see Theorem 3.1 in [21, Chapter 2].

In fact, one can show (we shall not need this) that already the principal divisors $(u_{\mathbf{a}})$, where \mathbf{a} runs through the set M_N , consisting of the elements of $(N^{-1}\mathbb{Z}/\mathbb{Z})^2$ of exact order N , generate a free abelian group of rank $\nu_{\infty}(N) - 1$. The number of such \mathbf{a} is $2\nu_{\infty}(N)$. It follows that, besides the relations $u_{\mathbf{a}} = u_{-\mathbf{a}}$, there can exist exactly one relation between the principal divisors $(u_{\mathbf{a}})$ with $\mathbf{a} \in M_N$. This relation is

$$\sum_{\mathbf{a} \in M_N} (u_{\mathbf{a}}) = 0.$$

In fact, we have a more precise statement:

$$\prod_{\mathbf{a} \in M_N} u_{\mathbf{a}} = \pm \Phi_N(1)^{12N}, \quad (16)$$

where $\Phi_N(t)$ is the N -th cyclotomic polynomial. In particular, if $N = p$ is a prime number, we obtain the following identity:

$$\prod_{\mathbf{a} \in M_p} u_{\mathbf{a}} = \pm p^{12p}. \quad (17)$$

(One can show that the sign is actually +.)

Let us prove (16). Since the set M_N is stable with respect to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the left-hand side of (16) is stable with respect to the Galois action over the field $\mathbb{Q}(X(1))$. Hence it is a unit on the curve $X(1)$, defined over \mathbb{Q} . Since $X(1)$ has only one cusp, it has no non-constant units. Hence the left-hand side of (16) is a constant belonging to \mathbb{Q} .

To determine the value of this constant, we evaluate it at the cusp at infinity. The left-hand side of (16) is a product of a root of unity and the terms of the type $(1 - e^{2\pi i a_2} q^{n+a_1})^{12N}$ and of the type $(1 - e^{2\pi i - a_2} q^{n+1-a_1})^{12N}$, where n runs through non-negative integers, and (a_1, a_2) runs through the lifting of the set M_N to the unit square $[0, 1)^2$. When we set $q = 0$, all these terms become 1 except the terms $(1 - e^{2\pi i a_2} q^{n+a_1})^{12N}$ with $n = 0$ and $a_1 = 0$. Hence, up to a root of unity, the left-hand side of (16) is

$$\prod_{\substack{a_2 \in N^{-1}\mathbb{Z}/\mathbb{Z} \\ a_2 \text{ is of order } N}} (1 - e^{2\pi i a_2})^{12N} = \prod_{\substack{0 \leq k < N \\ (k, N) = 1}} (1 - e^{2\pi i k/N})^{12N} = \Phi_N(1)^{12N}.$$

Since the only roots of unity in \mathbb{Q} are ± 1 , this proves (16).

4.3 Asymptotic Expansions

In this subsection we obtain several types of asymptotic expansions for the Siegel function. Our main tool will be the infinite product presentation (14). Recall (see Proposition 4.3) that $\mathrm{Ord}_q g_{\mathbf{a}} = \ell_{\mathbf{a}}$, where $\ell_{\mathbf{a}} = B_2(a_1 - \lfloor a_1 \rfloor)/2$. Clearly, $|\ell_{\mathbf{a}}| \leq 1/12$. We also put

$$\gamma_{\mathbf{a}} = \begin{cases} e^{\pi i a_2 (a_1 - 1)}, & a_1 \neq 0, \\ e^{\pi i a_2 (a_1 - 1)} (1 - e^{2\pi i a_2}), & a_1 = 0. \end{cases} \quad (18)$$

We start from a purely formal statement, by estimating the coefficients of a fractional power series representing the logarithm of (properly normalized) $g_{\mathbf{a}}$. In the sequel v is an absolute value of $\bar{\mathbb{Q}}$, extending a standard absolute value of \mathbb{Q} .

Proposition 4.7 *Let N be a denominator of \mathbf{a} . Then there exist $\beta_1, \beta_2, \beta_3 \dots \in \mathbb{Q}(\zeta_N)$ such that*

$$\log \frac{g_{\mathbf{a}}(q)}{\gamma_{\mathbf{a}} q^{\ell_{\mathbf{a}}}} = \sum_{k=1}^{\infty} \beta_k q^{k/N},$$

and

$$|\beta_k|_v \leq \begin{cases} |k|_v^{-1}, & v \mid p < \infty, \\ 2k/N + 2, & v \mid \infty \end{cases} \quad (k = 1, 2, \dots). \quad (19)$$

Proof We may assume that $0 \leq a_1 < 1$. For a fixed non-negative integer n (where we assume $n > 0$ if $a_1 = 0$) write

$$\log(1 - e^{2\pi i a_2} q^{n+a_1}) = \sum_{k=1}^{\infty} \alpha_k q^{k/N},$$

An immediate verification shows that $\alpha_k \in \mathbb{Q}(\zeta_N)$ and

$$|\alpha_k|_v \leq \begin{cases} |k|_v^{-1}, & v \text{ finite,} \\ 1, & v \text{ infinite} \end{cases} \quad (k = 1, 2, \dots).$$

Same estimates hold true for the coefficients of the q -series for $\log(1 - e^{2\pi i a_2} q^{n+1-a_1})$.

Coefficients of at most $k/N + 1$ series for $\log(1 - e^{2\pi i a_2} q^{n+a_1})$ (those with $0 \leq n \leq k/N$) may contribute to β_k , and the same is true for the series for $\log(1 - e^{2\pi i a_2} q^{n+1-a_1})$. The result now follows by summation. \square

We can now replace the infinite sum by a finite and estimate the error term, but the estimate would be very poor when $q^{1/N}$ is close to 1. To solve this problem, we take away one logarithmic term.

Proposition 4.8 1. In the set-up of Proposition 4.7 assume that $0 < a_1 < 1$ and put

$$(a'_1, a'_2) = \begin{cases} (a_1, a_2), & 0 < a_1 < 1/2, \\ (1 - a_1, -a_2), & 1/2 \leq a_1 < 1. \end{cases}$$

Then with a suitable choice of the logarithms and for $|q| < 0.0044$ we have

$$\log \frac{g_{\mathbf{a}}(q)}{\gamma_{\mathbf{a}} q^{\ell_{\mathbf{a}}}} = \log(1 - q^{a'_1} e^{2\pi i a'_2}) + O_1(1.2|q|^{1/2}). \quad (20)$$

Further, there exist $\beta'_1, \beta'_2, \beta'_3 \dots \in \mathbb{Q}(\zeta_N)$ such that the following holds. Let ν be a non-negative integer. Then with a suitable choice of the logarithms and for $|q| < 0.0044$ we have

$$\log \frac{g_{\mathbf{a}}(q)}{\gamma_{\mathbf{a}} q^{\ell_{\mathbf{a}}}} = \log(1 - q^{a'_1} e^{2\pi i a'_2}) + \sum_{k=1}^{\nu} \beta'_k q^{k/N} + O_1((2.2\nu/N + 3.1)|q|^{(\nu+1)/N}). \quad (21)$$

2. When $a_1 = 0$ we have

$$\log \frac{g_{\mathbf{a}}(q)}{\gamma_{\mathbf{a}} q^{\ell_{\mathbf{a}}}} = O_1(2.02|q|).$$

Also, an analog of (21) holds true with $\beta'_k = \beta_k$ and without the additional logarithmic term on the right:

$$\log \frac{g_{\mathbf{a}}(q)}{\gamma_{\mathbf{a}} q^{\ell_{\mathbf{a}}}} = \sum_{k=1}^{\nu} \beta_k q^{k/N} + O_1((2.2\nu/N + 3.1)|q|^{(\nu+1)/N}).$$

(Estimates similar to (19) hold for the numbers β'_k as well but we shall not need them.)

Proof For $|z| \leq r < 1$ and non-negative integer m we have

$$\log(1 - z) = - \sum_{k=1}^m \frac{z^k}{k} + O_1\left(\frac{|z|^{m+1}}{1-r}\right). \quad (22)$$

(This estimate is very rough but sufficient for us.)

Assume, for instance, that $0 < a_1 < 1/2$, so that $(a'_1, a'_2) = (a_1, a_2)$. Let n be a positive integer. Then we have

$$\log \frac{g_{\mathbf{a}}(q)}{\gamma_{\mathbf{a}} q^{\ell_{\mathbf{a}}}} = \sum_{k=0}^{n-1} (\log(1 - q^{k+a_1} e^{2\pi i a_2}) + \log(1 - q^{k+1-a_1} e^{-2\pi i a_2})) + O_1(2.02|q|^{n+a_1}). \quad (23)$$

To prove (23) we have to estimate the sum

$$\sum_{k=n+1}^{\infty} (|\log(1 - q^{k+a_1} e^{2\pi i a_2})| + |\log(1 - q^{k+1-a_1} e^{-2\pi i a_2})|).$$

Applying (22) with $m = 0$ and $r = 0.0044$ to each term of the latter sum, we estimate the sum as

$$1.0045 \frac{|q|^{n+a_1} + |q|^{n+1-a_1}}{1 - |q|} \leq 1.01(|q|^{n+a_1} + |q|^{n+1-a_1}) \leq 2.02|q|^{n+a_1},$$

because $n+1-a_1 \geq n+a_1$. This proves (23).

Now to establish (20) we take $n = 1$. We obtain

$$\log \frac{g_{\mathbf{a}}(q)}{\gamma_{\mathbf{a}} q^{\ell_{\mathbf{a}}}} = \log(1 - q^{a_1} e^{2\pi i a_2}) + \log(1 - q^{1-a_1} e^{-2\pi i a_2}) + O_1(2.02|q|).$$

Since $a_1 < 1/2$, we have $|q^{1-a_1}| \leq |q|^{1/2} \leq 0.067$. Applying (22) with $m = 0$ and $r = 0.067$, we obtain (20).

$$\begin{aligned} \log \frac{g_{\mathbf{a}}(q)}{\gamma_{\mathbf{a}} q^{\ell_{\mathbf{a}}}} &= \log(1 - q^{a_1} e^{2\pi i a_2}) + O_1(1.072|q|^{1/2} + 2.02|q|) \\ &= \log(1 - q^{a_1} e^{2\pi i a_2}) + O_1(1.2|q|^{1/2}), \end{aligned}$$

proving (20).

To prove (21) we define n as the smallest integer such that $n + a_1 > \nu/N$. Now, for $k \geq 1$ we have $|q^{k+a_1}| \leq |q| \leq 0.0044$, and for $k \geq 0$ we have $|q^{k+1-a_1}| \leq |q|^{1/2} \leq 0.067$. Applying (22) with $r = 0.067$ and with suitable m to each logarithmic term of the right-hand side of (23) except the term $\log(1 - q^{a_1} e^{2\pi i a_2})$, we obtain (21) with the error term $(1.08(2n-1) + 2.02)q^{(\nu+1)/N}$. Since $n \leq \nu/N + 1$, the latter quantity is bounded by $(2.2\nu/N + 3.1)q^{(\nu+1)/N}$, as wanted.

In a similar way one treats the case $1/2 \leq a_1 < 1$, but now the term $\log(1 - q^{1-a_1} e^{-2\pi i a_2})$ must be excluded.

In the case $a_1 = 0$ the proofs are similar and simpler, and we omit them. \square

When $|q|^{1/N}$ is small enough, the extra term can be omitted as well.

Corollary 4.9 *In the set-up of Proposition 4.7 assume that $|q| \leq 2^{-N}$. Then*

$$\log \frac{g_{\mathbf{a}}(q)}{\gamma_{\mathbf{a}} q^{\ell_{\mathbf{a}}}} = O_1(3.2|q|^{1/N}), \quad (24)$$

$$\log \frac{g_{\mathbf{a}}(q)}{\gamma_{\mathbf{a}} q^{\ell_{\mathbf{a}}}} = \sum_{k=1}^{\nu} \beta_k q^{k/N} + O_1((2.2\nu/N + 5.1)q^{(\nu+1)/N}). \quad (25)$$

Proof We may assume that $0 < a_1 < 1$ and combine (20) or (21) with (22). \square

5 General Modular Units

In this section we review and complement some of the results of Kubert and Lang [21]. Our purpose is to construct “economical” modular units on the curve X_G .

The “naive” way to do is as follows. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and H a subgroup of $\det G$, which itself is a subgroup in $(\mathbb{Z}/N\mathbb{Z})^\times$, viewed as the Galois group of the cyclotomic field $\mathbb{Q}(\zeta_N)$. Then H left-acts naturally on the set of the cusps of X_G . Denote by $\nu_\infty(G)$ the number of cusps and by $\nu_\infty(G, H)$ the number H -orbits of cusps.

On the other hand, the group G_H , defined in (3), right-acts on the set $(N^{-1}\mathbb{Z}/\mathbb{Z})^2$. If $\mathcal{O} \subset (N^{-1}\mathbb{Z}/\mathbb{Z})^2$ is a non-zero orbit of this action, then

$$\prod_{\mathbf{a} \in \mathcal{O}} u_{\mathbf{a}} \quad (26)$$

is a rational function on the curve X_G defined over the field $\mathbb{Q}(\zeta_N)^H$.

It is not difficult to deduce from Theorem 4.6 that the principal divisors defined by products (26), where \mathcal{O} runs the non-zero G_H -orbits, generate a free abelian group whose rank is $\nu_\infty(G, H) - 1$.

Product (26) can be written as

$$\prod_{\mathbf{a} \in \mathcal{O}} g_{\tilde{\mathbf{a}}}^{12N}, \quad (27)$$

where $\tilde{\mathbf{a}} \in N^{-1}\mathbb{Z}^2$ is a lifting of $\mathbf{a} \in (N^{-1}\mathbb{Z}/\mathbb{Z})^2$. It turns out that in many interesting cases the exponents $12N$ can be considerably reduced, which is important for numerical purposes. This is the principal goal of this section.

5.1 Quadratic Relations

Let N be a positive integer. We have the natural group isomorphism $(N^{-1}\mathbb{Z}/\mathbb{Z})^2 \cong (\mathbb{Z}/N\mathbb{Z})^2$, and, with some abuse of speech, we identify the two groups. In particular, for $\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2$ we have the corresponding element in $(N^{-1}\mathbb{Z}/\mathbb{Z})^2$, and for this latter we may fix a lifting in $N^{-1}\mathbb{Z}^2$, which will be called a lifting of \mathbf{a} to $N^{-1}\mathbb{Z}^2$. By a lifting of a set $A \subset (\mathbb{Z}/N\mathbb{Z})^2$ we mean a mapping $A \rightarrow N^{-1}\mathbb{Z}^2$ such that for every $\mathbf{a} \in A$ its image $\tilde{\mathbf{a}} \in N^{-1}\mathbb{Z}^2$ is a lifting of \mathbf{a} in the sense defined above.

Our principal tool will be the following result of Kubert and Lang [21], see Theorem 5.2 in Chapter 3.

Theorem 5.1 *To every non-zero $\mathbf{a} = (a_1, a_2) \in (\mathbb{Z}/N\mathbb{Z})^2$ we associate an integer $m(\mathbf{a})$. Fix a lifting $\mathbf{a} \mapsto \tilde{\mathbf{a}}$ of the set of non-zero elements of $(\mathbb{Z}/N\mathbb{Z})^2$. Put*

$$\Lambda = \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} m(\mathbf{a}). \quad (28)$$

1. Assume that N is odd. Then

$$\prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} \mathfrak{t}_{\tilde{\mathbf{a}}}^{m(\mathbf{a})} \quad (29)$$

is $\Gamma(N)$ -automorphic (of level $-\Lambda$) if and only if

$$\sum_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} m(\mathbf{a}) a_1^2 = \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} m(\mathbf{a}) a_2^2 = \sum_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} m(\mathbf{a}) a_1 a_2 = 0. \quad (30)$$

2. Assume that $\gcd(N, 6) = 1$. Then the function

$$\prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} g_{\tilde{\mathbf{a}}}^{m(\mathbf{a})} \quad (31)$$

is $\Gamma(N)$ -automorphic (of level 0) if and only if (30) holds and $12 \mid \Lambda$.

Remark 5.2 1. Kubert and Lang call (30) “quadratic relations” (modulo N).

2. One may notice that

$$\prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} g_{\tilde{\mathbf{a}}}^{m(\mathbf{a})} = \prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} \mathfrak{t}_{\tilde{\mathbf{a}}}^{m(\mathbf{a})} \cdot \Delta^{\Lambda/12}, \quad (32)$$

where $\Delta = \eta^{24}$.

3. The assumption $\gcd(N, 6) = 1$ is purely technical: in a slightly modified form the statement holds true when N is divisible by 2 and/or by 3. However, assuming that $\gcd(N, 6) = 1$ will not hurt us, since we shall apply Theorem 5.1 only when N is prime and $N \geq 7$.
4. Theorem 5.1 implies that product (31) defines a function $f \in \mathbb{C}(X(N))$. By considering the q -expansion, as in Subsection 4.2, we conclude that in fact $f \in \mathbb{Q}(\zeta_N)(X(N))$.

Contrary to product (27), product (31) may depend on the choice of the lifting $\mathbf{a} \mapsto \tilde{\mathbf{a}}$. Proposition 4.1:3 implies that if we choose a different lifting $\mathbf{a} \mapsto \tilde{\mathbf{a}}'$ then (29) and (31) will be multiplied by a $2N$ -th root of unity. Though this is pretty trivial, we state this as a proposition for further reference.

Proposition 5.3 For every non-zero $\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2$ pick an integer $m(\mathbf{a})$ and fix **two** liftings $\mathbf{a} \mapsto \tilde{\mathbf{a}}$ and $\mathbf{a} \mapsto \tilde{\mathbf{a}}'$ of the set of non-zero elements of $(\mathbb{Z}/N\mathbb{Z})^2$. Then there exists a $2N$ -th root of unity ε such that

$$\prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} \mathfrak{t}_{\tilde{\mathbf{a}}'}^{m(\mathbf{a})} = \varepsilon \prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} \mathfrak{t}_{\tilde{\mathbf{a}}}^{m(\mathbf{a})}. \quad (33)$$

If, in addition, $12 \mid \Lambda$, where Λ defined in (28), then

$$\prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} g_{\tilde{\mathbf{a}}'}^{m(\mathbf{a})} = \varepsilon \prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} g_{\tilde{\mathbf{a}}}^{m(\mathbf{a})}. \quad (34)$$

If every $2 \mid m(\mathbf{a})$ for every \mathbf{a} then

$$\varepsilon^N = 1. \quad (35)$$

Proof Statements (33) and (35) follow from Proposition 4.1:3, and (34) follows from (33) and (32). \square

5.2 Galois Action

As we mentioned in Subsection 4.2, the Galois action by the group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the “simplest” modular units $u_{\mathbf{a}} = g_{\tilde{\mathbf{a}}}^{12N}$ is very easy to describe: it is given by relation (15). We want to obtain a similar result for “general” modular units (31).

Proposition 5.4 Assume the set-up of item 2 of Theorem 5.1, so that

$$f = \prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} g_{\tilde{\mathbf{a}}}^{m(\mathbf{a})}$$

defines a function in $\mathbb{Q}(\zeta_N)(X_G)$ (see item 4 in Remark 5.2).

1. Assume that $\sigma \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and let $\tilde{\sigma}$ be a lifting of σ to $\Gamma(1)$. Then

$$f^\sigma = \prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} g_{\tilde{\mathbf{a}}\tilde{\sigma}}^{m(\mathbf{a})}. \quad (36)$$

2. Assume that $\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then it has a lifting $\tilde{\sigma} \in \mathrm{M}_2(\mathbb{Z})$ such that (36) holds.

Proof Item 1 is a consequence of Proposition 2.1:1, Proposition 4.1:2 and (32). Indeed, write $\tilde{\sigma} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and recall that $\Delta = \eta^{24}$ is $\Gamma(1)$ -automorphic of weight 12. We obtain:

$$\begin{aligned} f^\sigma(\tau) &= f \circ \tilde{\sigma}(\tau) \\ &= \prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} (\mathfrak{k}_{\tilde{\mathbf{a}}} \circ \tilde{\sigma}(\tau))^{m(\mathbf{a})} \cdot (\Delta \circ \tilde{\sigma}(\tau))^{\Lambda/12} \\ &= (c\tau + d)^{-\Lambda} \prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} \mathfrak{k}_{\tilde{\mathbf{a}}\tilde{\sigma}}(\tau)^{m(\mathbf{a})} \cdot (c\tau + d)^\Lambda \Delta(\tau)^{\Lambda/12} \\ &= \prod_{\substack{\mathbf{a} \in (\mathbb{Z}/N\mathbb{Z})^2 \\ \mathbf{a} \neq 0}} g_{\tilde{\mathbf{a}}\tilde{\sigma}}(\tau)^{m(\mathbf{a})}, \end{aligned}$$

as wanted.

In the proof of item 2 we may assume that σ is of the form $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, because any $\sigma \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ can be presented as $\sigma_1\sigma_2$ with $\sigma_1 \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and σ_2 of this form. We lift $\sigma = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ as $\tilde{\sigma} = \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, and the result follows immediately from Proposition 2.1:3 and infinite product (14). \square

5.3 “Economical” Modular Units on X_G

In this subsection, to avoid technicalities, we restrict to the prime level. Thus, let p be a prime number, G a subgroup in $\mathrm{GL}_2(\mathbb{F}_p)$ and H a subgroup in $\det G$. The group G_H , defined in (3), right-acts on the set $M_p = \mathbb{F}_p^2 \setminus \{0\}$ (as in the previous subsection, we tacitly identify the sets \mathbb{F}_p^2 and $(p^{-1}\mathbb{Z}/\mathbb{Z})^2$). Let $\mathcal{O} \subset M_p$ be an orbit of this action, or, more generally, a G_H -invariant subset of M_p . We fix a lifting $\mathbf{a} \mapsto \tilde{\mathbf{a}}$ of the set \mathcal{O} (as defined in the beginning of Subsection 5.1) and want to find an exponent m such that

$$\prod_{\mathbf{a} \in \mathcal{O}} g_{\tilde{\mathbf{a}}}^m \quad (37)$$

defines a function in $K(X_G)$, where $K = \mathbb{Q}(\zeta_p)^H$. Clearly, $m = 12p$ would do. It turns out that in some cases one can do much better, sometimes introducing a root of unity factor. We fix a p -th primitive root of unity and denote it by ζ_p .

Theorem 5.5 *Let $p \geq 5$ be a prime number and $G \ni -I$ a semi-simple subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ (with is equivalent to saying that $|G|$ is not divisible by p). Let H be a subgroup of $\det G$ and $\mathcal{O} \subset M_p$ a G_H -invariant subset of M_p satisfying*

$$\sum_{\mathbf{a} \in \mathcal{O}} a_1^2 = \sum_{\mathbf{a} \in \mathcal{O}} a_1 a_2 = \sum_{\mathbf{a} \in \mathcal{O}} a_2^2. \quad (38)$$

Let m be an integer such that

$$2 \mid m, \quad 12 \mid m|\mathcal{O}|. \quad (39)$$

Fix a lifting $\mathbf{a} \mapsto \tilde{\mathbf{a}}$ of the set \mathcal{O} and denote by f product (37). Then f defines a function in $\mathbb{Q}(\zeta_p)(X_G)$ (denoted by f as well). Further, there exists $k \in \mathbb{Z}$ (which is unique mod p when $H \neq 1$) such that $\zeta_p^k f \in K(X_G)$, where $K = \mathbb{Q}(\zeta_p)^H$.

The proof requires a lemma, which is the simplest special case of Kummer’s theory (see any textbook in algebra).

Lemma 5.6 *Let p be a prime number and F a field of characteristic distinct from p . Let α be an element in the algebraic closure \bar{F} , and $\zeta_p \in \bar{F}$ a primitive p -th root of unity. Assume that $\alpha^p \in F$. Then either $[F(\alpha) : F] = p$ or there exists $k \in \mathbb{Z}$ (which is unique mod p when $\zeta_p \notin F$) such that $\zeta_p^k \alpha \in F$. In particular, if $\zeta_p \in F$ then either $[F(\alpha) : F] = p$ or $\alpha \in F$.*

Proof of Theorem 5.5 Theorem 5.1 (together with item 4 of Remark 5.2) implies that f defines a function in $\mathbb{Q}(\zeta_p)(X(p))$. We want to study the Galois action of G_H on f . Thus, fix $\sigma \in G_H$. Proposition 5.4:2 implies that there exists a lifting $\tilde{\sigma} \in M_2(\mathbb{Z})$ such that

$$f^\sigma = \prod_{\mathbf{a} \in \mathcal{O}} g_{\tilde{\mathbf{a}}\tilde{\sigma}}^m. \quad (40)$$

Since \mathcal{O} is G_H -invariant, we have $\mathcal{O}\sigma^{-1} = \mathcal{O}$. Consider a different lifting $\mathbf{a} \mapsto \tilde{\mathbf{a}}'$ of \mathcal{O} defined by $\tilde{\mathbf{a}}' = \mathbf{a}\sigma^{-1}\tilde{\sigma}$, where $\mathbf{a}\sigma^{-1}$ is the lifting of $\mathbf{a}\sigma^{-1}$. Then (40) can be re-written as

$$f^\sigma = \prod_{\mathbf{a} \in \mathcal{O}} g_{\tilde{\mathbf{a}}'}^m.$$

Now Proposition 5.3 implies that f^σ/f is a p -th root of unity. We have proved that f^p is invariant under the Galois action by G_H , which implies that $f^p \in K(X_G)$, the G_H -invariant subfield of $\mathbb{Q}(\zeta_p)(X(p))$. Now Lemma 5.6 completes the proof. \square

There is an important special case when f itself belongs to $K(X_G)$, without multiplication by a root of unity. Assume that G_H contains $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. In this case $\mathbf{a} = (a_1, a_2)$ belongs to a G_H -orbit \mathcal{O} if and only if its “complex conjugate” $\bar{\mathbf{a}} = (a_1, -a_2)$ does. We say that a lifting $\mathbf{a} \mapsto \tilde{\mathbf{a}}$ respects the complex conjugation if the following holds: if $\mathbf{a} = (a_1, a_2) \in \mathcal{O}$ is lifted to $\tilde{\mathbf{a}} = (\tilde{a}_1, \tilde{a}_2)$, then the lifting of $\bar{\mathbf{a}}$ is $(\tilde{a}_1, -\tilde{a}_2)$. This can be expressed briefly as $\tilde{\bar{\mathbf{a}}} = \bar{\tilde{\mathbf{a}}}$.

Corollary 5.7 *In the set-up of Theorem 5.5 assume that $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in G_H$ and the lifting respects the complex conjugation. Then $f \in K(X_G)$.*

Proof The assumption $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in G_H$ implies that $K \subseteq \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$. Further, since the lifting respects the complex conjugation, we have $f^\iota = f$, where $\iota = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The subfield of $\mathbb{Q}(\zeta_p)(X_G)$ stabilized by ι is $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)(X_G)$. Thus, $f \in \mathbb{Q}(\zeta_p + \bar{\zeta}_p)(X_G)$ and $\zeta_p^k f \in K(X_G)$ with $K \subseteq \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$. It follows that $\zeta_p^k \in \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ which is only possible if $\zeta_p^k = 1$. \square

5.4 An Example

We conclude this section with an example. It will not be used in the sequel, but it gives a good illustration of how Theorem 5.5 can be used.

We take as G the diagonal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ and set $H = \{1, -1\}$, so that

$$G_H = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : ad = \pm 1 \right\}$$

and $K = \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$.

There are $(p-1)/2$ orbits, which are of the form $\{\mathbf{a} : a_1 a_2 = \pm c\}$ with $c = 1, \dots, (p-1)/2$. Quadratic relations (38) are clearly satisfied, and to have (39) it suffices to take

$$m = \begin{cases} 2, & p \equiv 1 \pmod{3}, \\ 6, & p \equiv -1 \pmod{3}. \end{cases}$$

Selecting a lifting respecting the complex conjugation, we obtain $(p-1)/2$ modular units in the field $K(X_G)$.

6 Cusp Points and Units on $X_{\mathrm{ns}}^+(p)$

From now on we restrict to the case when $N = p$ is a prime number and G is the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. A very detailed account of various properties of this curve (even for an arbitrary N) can be found in Sections 3 and 6 of Baran’s article [5].

We may and will assume that

$$G = \left\{ \begin{pmatrix} \alpha & \Xi\beta \\ \beta & \alpha \end{pmatrix}, \begin{pmatrix} \alpha & \Xi\beta \\ -\beta & -\alpha \end{pmatrix} : \alpha, \beta \in \mathbb{F}_p, (\alpha, \beta) \neq (0, 0) \right\}, \quad (41)$$

where Ξ is a quadratic non-residue modulo p , which will be fixed from now on. In particular, one can take $\Xi = -1$ if $p \equiv 3 \pmod{4}$.

We fix, until the end of the article, a lifting $\mathbf{a} \mapsto \tilde{\mathbf{a}}$ of the set M_p to $p^{-1}\mathbb{Z}^2$, which respects the complex conjugation (as defined before Corollary 5.7) and, in addition to this, has the following property:

$$\text{if } \tilde{\mathbf{a}} = (\tilde{a}_1, \tilde{a}_2) \text{ is a lifting of } \mathbf{a} \in M_p \text{ then } 0 \leq \tilde{a}_1 < 1. \quad (42)$$

6.1 Cusps

The curve $X_G = X_{\text{ns}}^+(p)$ has $(p-1)/2$ cusps, defined over the real cyclotomic fields $\mathbb{Q}(\zeta_p + \bar{\zeta}_p)$, and the Galois group $\text{Gal}(\mathbb{Q}(\zeta_p + \bar{\zeta}_p)/\mathbb{Q}) = \mathbb{F}_p/\{\pm 1\}$ acts transitively on the cusps.

According to Remark 2.2, the cusps stay in one-to-one correspondence with the orbits of the left G_1 -action on the set $M_p = \mathbb{F}_p^2 \setminus \{(0, 0)\}$. These orbits are the sets defined by $x^2 - \Xi y^2 = \pm c$, where c runs through (representatives of) cosets $\mathbb{F}_p^\times/\{\pm 1\}$, the cusp at infinity corresponding to $c = 1$.

For every $c \in \mathbb{F}_p^\times/\{\pm 1\}$ fix $(a, b) \in \mathbb{F}_p^2$ such that $a^2 - \Xi b^2 = c^{-1}$ and let σ_c be a lifting to $\Gamma(1)$ of the matrix $\begin{pmatrix} ca & b\Xi \\ cb & a \end{pmatrix}$. For $c = 1$ we take $(a, b) = (1, 0)$ and $\sigma_1 = I$. Then the set $\{\sigma_c(i\infty) : c \in \mathbb{F}_p^\times/\{\pm 1\}\}$ is a full system of representatives of cusps on $\bar{\mathcal{H}}$. We can complete the set $\{\sigma_c : c \in \mathbb{F}_p^\times/\{\pm 1\}\}$ to an optimal system of representatives of cosets of $\Gamma_{\text{ns}}^+ \backslash \Gamma(1)$, as explained in Subsection 2.1.

In the sequel we fix a subgroup H of \mathbb{F}_p^\times , containing -1 and put $d = [\mathbb{F}_p^\times : H]$. In particular,

$$d = [K : \mathbb{Q}],$$

where $K = \mathbb{Q}(\zeta_p)^H$. The group H acts on the set of cusps by Galois conjugation, and this action has exactly d orbits, each of them being defined over K as a set. The Galois group $\text{Gal}(K/\mathbb{Q}) = \mathbb{F}_p^\times/H$ acts on the set of H -orbits transitively. These H -orbits of cusps are in one-to-one correspondence with the sets defined by $x^2 - \Xi y^2 \in cH$, with cH running through the cosets \mathbb{F}_p^\times/H .

6.2 Units

Besides the left action, the group G_H acts on the set M_p on the right. There are again d orbits of this action, and they are defined by $\Xi x^2 - y^2 \in cH$. These orbits will be used to define modular units in $K(X_G)$. Recall that we fixed a lifting $\mathbf{a} \mapsto \tilde{\mathbf{a}}$ of M_p to $p^{-1}\mathbb{Z}^2$, respecting the complex conjugation.

Theorem 6.1 *Let \mathcal{O} be right G_H -orbit on M_p . Pick a lifting $\mathbf{a} \mapsto \tilde{\mathbf{a}}$ of \mathcal{O} to $p^{-1}\mathbb{Z}^2$. Put*

$$m = \begin{cases} 2, & 3 \mid (p+1)|H|, \\ 6, & \text{otherwise.} \end{cases} \quad (43)$$

Then the product

$$u_{\mathcal{O}} = \prod_{\mathbf{a} \in \mathcal{O}} g_{\tilde{\mathbf{a}}}^m \quad (44)$$

is well-defined (depends only on the orbit \mathcal{O} but not on the particular lifting) and defines a function in $K(X_G)$.

We deduce this theorem from Theorem 5.5 (more precisely, from Corollary 5.7), using some elementary lemmas about finite fields. We thank Julia Baoulina for useful explanations and for the proof of Lemma 6.3 below.

Lemma 6.2 *Let $P(x_1, \dots, x_n) \in \mathbb{F}[x_1, \dots, x_n]$ be a polynomial over a finite field $\mathbb{F} = \mathbb{F}_q$ of degree $\deg P < n(q-1)$. Then*

$$\sum_{\mathbf{b} \in \mathbb{F}^n} P(\mathbf{b}) = 0.$$

Proof This is Lemma 6.4 in [24]. □

Lemma 6.3 *Let \mathbb{F} be a finite field of odd characteristic and having more than 3 elements. Further, let $f(x, y), g(x, y) \in \mathbb{F}[x, y]$ be quadratic forms over \mathbb{F} . Then for $c \in \mathbb{F}^\times$ we have*

$$\sum_{\substack{a, b \in \mathbb{F} \\ g(a, b) = \pm c}} f(a, b) = 0.$$

where the sum is over the couples $(a, b) \in \mathbb{F}^2$ such that $g(a, b) = \pm c$.

Proof Write $q = |\mathbb{F}|$, so that $\mathbb{F} = \mathbb{F}_q$. Then

$$\sum_{\substack{a, b \in \mathbb{F} \\ g(a, b) = \pm c}} f(a, b) = \sum_{a, b \in \mathbb{F}} f(a, b) (2 - (g(a, b) - c)^{q-1} - (g(a, b) + c)^{q-1}).$$

We have

$$f(x, y) (2 - (g(x, y) - c)^{q-1} - (g(x, y) + c)^{q-1}) = -2f(x, y)g(x, y)^{q-1} + \text{terms of degree } < 2(q-1),$$

and Lemma 6.2 implies that the wanted sum is equal to -2 times $\sum_{a, b \in \mathbb{F}} f(x, y)g(x, y)^{q-1}$. The latter sum is

$$\sum_{\substack{a, b \in \mathbb{F} \\ g(a, b) \neq 0}} f(a, b),$$

which, again by Lemma 6.2 and by the assumption $q > 3$ is equal to -1 times

$$\sum_{\substack{a, b \in \mathbb{F} \\ g(a, b) = 0}} f(a, b).$$

If the quadratic form $g(x, y)$ is anisotropic over \mathbb{F} then the latter sum consists only of the term $f(0, 0)$ and there is nothing to prove. And if it is isotropic then, after a variable change, we may assume that $g(x, y) = xy$. Writing $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$, the latter sum becomes $(\alpha + \gamma) \sum_{a \in \mathbb{F}} a^2$. Lemma 6.2 implies that $\sum_{a \in \mathbb{F}} a^2 = 0$ when \mathbb{F} has more than 3 elements. This completes the proof. □

Proof of Theorem 6.1 Recall that the orbit \mathcal{O} consists of $(x, y) \in \mathbb{F}_p^2$ satisfying $\Xi x^2 - y^2 \in cH$ with some $c \in \mathbb{F}_p^\times$. Since $H \ni -1$, Lemma 6.3 implies that the quadratic relations (38) hold true. Further, for each $c \in \mathbb{F}_p^\times$ there is exactly $p+1$ elements of \mathbb{F}_{p^2} of norm c , which implies that our orbit \mathcal{O} has exactly $(p+1)|H|$ elements, and with our choice of m the divisibility conditions (39) hold true as well. Corollary 5.7 now implies that $u \in K(X_G)$.

Finally, $u_{\mathcal{O}}$ does not depend on the lifting. Indeed, if we choose two different liftings respecting the complex conjugation and obtain the products, say, u and u' , then u/u' is a p -th root of unity by Proposition 5.3. On the other hand, $u, u' \in K(X_G)$, which implies that $u/u' \in K$, a totally real field. Hence $u = u'$. The theorem is proved. □

6.3 Asymptotics

Wi fix a right G_H -orbit \mathcal{O} . Using the results of Subsection 4.3, we may obtain two types of asymptotic expansions for the unit $u_{\mathcal{O}}$ defined in Subsection 6.2. Let c be a cusp of X_G . We define the set Ω_c and the q -parameter q_c as in Subsection 2.2, and with respect to the optimal system of representatives defined in Subsection 6.1: $q_c(\tau) = e^{2\pi i \sigma_c^{-1}(\tau)}$. Put

$$\gamma_c = \gamma_{c, \mathcal{O}} = \prod_{\mathbf{a} \in \mathcal{O}_{\sigma_c}} \gamma_{\mathbf{a}}^m, \quad (45)$$

where $\gamma_{\mathbf{a}}$ is defined in (18).

It follows from the definition of $\gamma_{\mathbf{a}}$ that $h(\gamma_{\mathbf{a}}) = 0$ if $a_1 \neq 0$ and $h(\gamma_{\mathbf{a}}) \leq \log 2$ if $a_1 = 0$. Hence

$$h(\gamma_{c, \mathcal{O}}) \leq (\log 2) |\{\mathbf{a} \in \mathcal{O} : a_1 = 0\}| \leq 2|H| \log 2. \quad (46)$$

Proposition 6.4 *Let c be cusp of X_G . Then for $k = 1, 2, \dots$ there exist algebraic numbers $\beta_{k,c}, \beta'_{k,c} \in \mathbb{Q}(\zeta_p)$ such that for any absolute value v of $\mathbb{Q}(\zeta_p)$ we have²*

$$|\beta_{k,c}|_v \leq \begin{cases} |k|_v^{-1}, & v \mid p < \infty, \\ 2m(p+1)|H|(k/N+1), & v \mid \infty \end{cases} \quad (k = 1, 2, \dots) \quad (47)$$

and the following holds. Let ν be a non-negative integer. Then for $P \in \Omega_c$ we have, with a suitable choice of logarithms,

$$\begin{aligned} \log \frac{u_{\mathcal{O}}(P)}{q_c^{\frac{\text{Ord}_c u_{\mathcal{O}}}{p} \gamma_c}} &= m \sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_c} \\ 0 < \tilde{a}_1 < 1/2}} \log(1 - q_c^{\tilde{a}_1} e^{2\pi i \tilde{a}_2}) + m \sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_c} \\ 1/2 \leq \tilde{a}_1 < 1}} \log(1 - q_c^{1-\tilde{a}_1} e^{-2\pi i \tilde{a}_2}) \\ &\quad + O_1 \left(1.2m(p+1)|H||q_c|^{1/2} \right) \\ \log \frac{u_{\mathcal{O}}(P)}{q_c^{\frac{\text{Ord}_c u_{\mathcal{O}}}{p} \gamma_c}} &= m \sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_c} \\ 0 < \tilde{a}_1 < 1/2}} \log(1 - q_c^{\tilde{a}_1} e^{2\pi i \tilde{a}_2}) + m \sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_c} \\ 1/2 \leq \tilde{a}_1 < 1}} \log(1 - q_c^{1-\tilde{a}_1} e^{-2\pi i \tilde{a}_2}) \\ &\quad + \sum_{k=1}^{\nu} \beta'_{k,c} q_c^{k/p} + O_1 \left(m(p+1)|H| (2.2\nu/p + 3.1) |q_c|^{(\nu+1)/p} \right) \end{aligned}$$

where here and below we write $q_c = q_c(P)$. If, in addition, $|q_c(P)| \leq 2^{-p}$ then

$$\log \frac{u_{\mathcal{O}}(P)}{q_c^{\frac{\text{Ord}_c u_{\mathcal{O}}}{p} \gamma_c}} = O_1 \left(3.2m(p+1)|H||q_c|^{1/p} \right), \quad (48)$$

$$\log \frac{u_{\mathcal{O}}(P)}{q_c^{\frac{\text{Ord}_c u_{\mathcal{O}}}{p} \gamma_c}} = \sum_{k=1}^{\nu} \beta_{k,c} q_c^{k/p} + O_1 \left(m(p+1)|H| (2.2\nu/p + 5.1) |q_c|^{(\nu+1)/p} \right). \quad (49)$$

Proof In the case $c = c_{\infty}$ this is an immediate consequence of the results of Subsection 4.3. In particular, the error terms from (21) and (25) and the archimedean part of the estimate (19) should be multiplied by $m(p+1)|H|$, because $u_{\mathcal{O}}$ is a product of exactly $m|\mathcal{O}|$ Siegel functions, and $|\mathcal{O}| = (p+1)|H|$. The general case is treated similarly, using the variable change $\tau \mapsto \sigma_c \tau$. \square

Taking the real parts, we obtain the following consequence.

²Similar estimates hold for the numbers $\beta'_{k,c}$ as well, but we shall not need them.

Corollary 6.5 *In the set-up of Proposition 6.4 we have*

$$\begin{aligned} \log |u_{\mathcal{O}}(P)| &= \frac{\text{Ord}_c u_{\mathcal{O}}}{p} \log |q_c| + \log |\gamma_c| \\ &\quad + m \sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_c} \\ 0 < \tilde{a}_1 < 1/2}} \log |1 - q_c^{\tilde{a}_1} e^{2\pi i \tilde{a}_2}| + m \sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_c} \\ 1/2 \leq \tilde{a}_1 < 1}} \log |1 - q_c^{1-\tilde{a}_1} e^{-2\pi i \tilde{a}_2}| \\ &\quad + O_1 \left(1.2m(p+1)|H||q_c|^{1/2} \right) \end{aligned} \quad (50)$$

If $|q_c(P)| \leq 2^{-p}$ then we also have

$$\log |u_{\mathcal{O}}(P)| = \frac{\text{Ord}_c u_{\mathcal{O}}}{p} \log |q_c| + O_1 \left(3.2m(p+1)|H||q_c|^{1/p} \right). \quad (51)$$

If $q_c(P) \in \mathbb{R}$ and ν is a positive integer then we also have

$$\begin{aligned} \log |u_{\mathcal{O}}(P)| &= \frac{\text{Ord}_c u_{\mathcal{O}}}{p} \log |q_c| + \log |\gamma_c| \\ &\quad + m \sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_c} \\ 0 < \tilde{a}_1 < 1/2}} \log |1 - q_c^{\tilde{a}_1} e^{2\pi i \tilde{a}_2}| + m \sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_c} \\ 1/2 \leq \tilde{a}_1 < 1}} \log |1 - q_c^{1-\tilde{a}_1} e^{-2\pi i \tilde{a}_2}| \\ &\quad + \sum_{k=1}^{\nu} \text{Re}(\beta'_{k,c}) q_c^{k/p} + O_1 \left(m(p+1)|H| (2.2\nu/p + 3.1) |q_c|^{(\nu+1)/p} \right). \end{aligned} \quad (52)$$

We complete this subsection by estimating the orders of $u_{\mathcal{O}}$ at the cusps, and its degree as a rational function on X_G . Clearly,

$$\text{Ord}_c u_{\mathcal{O}} = pm \sum_{\mathbf{a} \in \mathcal{O}_{\sigma_c}} \ell_{\mathbf{a}},$$

where $\ell_{\mathbf{a}}$ is defined in Proposition 4.3. Since $|\ell_{\mathbf{a}}| \leq 1/12$, this has the following consequence, to be used in Section 8.

Proposition 6.6 *For any cusp c we have $\text{Ord}_c u_{\mathcal{O}} \leq \frac{1}{12}mp(p+1)|H|$. The degree of $u_{\mathcal{O}}$ as a rational function on X_G does not exceed $\frac{1}{48}mp(p^2-1)|H|$.*

6.4 Galois Action on the Units

Consider first the case of general algebraic curves. The proof of the following proposition is a standard exercise in Galois theory.

Proposition 6.7 *Let K/k be a finite Galois extension of fields of characteristic 0, and let X be a projective curve defined (that is, having a geometrically irreducible model) over k . Then the extension $K(X)/k(X)$ is Galois, and the restriction map*

$$\text{Gal}(K(X)/k(X)) \rightarrow \text{Gal}(K/k), \quad \sigma \mapsto \sigma|_K$$

defines isomorphism of Galois groups. Further, for $P \in X(k)$ and $f \in K(X)$ we have $f(P) \in K$, and given $\sigma \in \text{Gal}(K(X)/k(X)) = \text{Gal}(K/k)$, we have $f^{\sigma}(P) = f(P)^{\sigma}$.

In our case the group

$$\text{Gal}(K(X_G)/\mathbb{Q}(X_G)) = \text{Gal}(K/\mathbb{Q}) = G/G_H = \mathbb{F}_p^{\times}/H$$

acts transitively and faithfully on the right G_H -orbits, and this action agrees with the Galois action: for $\sigma \in \text{Gal}(K/\mathbb{Q}) = \mathbb{F}_p^{\times}/H$ we have $u_{\mathcal{O}}^{\sigma} = u_{\mathcal{O}\sigma}$. Fixing an orbit \mathcal{O} and putting $U = u_{\mathcal{O}}$, we obtain the following.

Proposition 6.8 For $P \in X_G(\mathbb{Q})$ we have $U(P) \in K$ and $U^\sigma(P) = U(P)^\sigma$ for $\sigma \in \text{Gal}(K/\mathbb{Q})$.

Since distinct orbits are disjoint, Theorem 4.6 and the discussion thereafter have the following consequence (recall that $d = [K : \mathbb{Q}] = [\mathbb{F}_p^\times : H]$).

Proposition 6.9 The d principal divisors (U^σ) , where $\sigma \in \text{Gal}(K/\mathbb{Q})$, generate an abelian group of rank $d - 1$, the only relation being $\sum_\sigma (U^\sigma) = 0$. In particular, if $d \geq 3$ and $\sigma \neq 1$ then U and U^σ are multiplicatively independent modulo the constants.

Finally, equation (17) implies that

$$\prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} U^\sigma = \pm p^m \quad (53)$$

7 The Principal Relation

We retain the set-up of Section 6 and, in particular, of Subsection 6.4:

- $p \geq 5$ is a prime number, ζ_p is a primitive p -th root of unity;
- $\mathbf{a} \mapsto \tilde{\mathbf{a}}$ is a lifting of the set $M_p = \mathbb{F}_p^2 \setminus \{(0,0)\}$ which respects the complex conjugation and satisfies (42);
- G is the normalizer of a non-split Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$, realized as in (41);
- H is a subgroup of \mathbb{F}_p^\times , $H \ni -1$;
- $m = 2$ or 6 according to (43).
- $K = \mathbb{Q}(\zeta_p)^H$, $d = [K : \mathbb{Q}] = [\mathbb{F}_p^\times : H]$;
- \mathcal{O} is a fixed right G_H -orbit in $M_p = \mathbb{F}_p \setminus \{0,0\}$, $U = u_{\mathcal{O}}$ as defined in Theorem 6.1.

We fix a system $\eta_1, \dots, \eta_{d-1}$ of fundamental units of the field K . We also put

$$\eta_0 = \mathcal{N}_{\mathbb{Q}(\zeta_p)/K}(1 - \zeta_p). \quad (54)$$

Clearly,

$$h(\eta_0) \leq |H| \log 2. \quad (55)$$

Also, η_0 generates the prime ideal \mathfrak{p} of K above p ; recall that $\mathfrak{p}^d = (p)$.

Recall that we call a point $P \in X_G(\mathbb{Q})$ *integral* if $j(P) \in \mathbb{Z}$. Proposition 4.5 implies that for an integral point P on X_G , the principal ideal $(U(P))$ is an integral ideal of the field K , and, moreover, it is a power of \mathfrak{p} . Since $\mathfrak{p}^\sigma = \mathfrak{p}$ for $\sigma \in \text{Gal}(K/\mathbb{Q})$, relation (53) implies that $(U(P)) = \mathfrak{p}^m$. Thus, we have

$$U(P) = \pm \eta_0^{b_0} \eta_1^{b_1} \dots \eta_{d-1}^{b_{d-1}}, \quad (56)$$

where $b_0 = m$ and b_1, \dots, b_{d-1} are some rational integers depending on P .

The purpose of this section is to express the exponents b_k in terms of the point P ; more precisely, in terms of $q_c(P)$, where c is the nearest cusp to P (Subsection 2.2). This can be viewed as an analogue of equation (20) on page 378 of [7].

For $\sigma \in \text{Gal}(K/\mathbb{Q})$ we have

$$U^\sigma(P) = \pm (\eta_0^\sigma)^{b_0} (\eta_1^\sigma)^{b_1} \dots (\eta_{d-1}^\sigma)^{b_{d-1}}.$$

Fix an ordering on the elements of the Galois group: $\text{Gal}(K/\mathbb{Q}) = \{\sigma_0 = \text{id}, \sigma_1, \dots, \sigma_{d-1}\}$. Since the real algebraic numbers $\eta_0, \eta_1, \dots, \eta_{d-1}$ are multiplicatively independent, the $d \times d$ real matrix $(\log |\eta_\ell^{\sigma_k}|)_{0 \leq k, \ell \leq d-1}$ is non-singular. Let $(\alpha_{k\ell})_{0 \leq k, \ell \leq d-1}$ be the inverse matrix. Then

$$b_k = \sum_{\ell=0}^{d-1} \alpha_{k\ell} \log |U^{\sigma_\ell}(P)| \quad (k = 0, 1, \dots, d-1). \quad (57)$$

Now, combining (57) with Corollary 6.5, we may express b_k in terms of P . Let us introduce some notation. Let c be a cusp of X_G , and q_c is the corresponding q -parameter (with respect to the optimal system of representatives defined in Subsection 6.1). Define the following quantities:

$$\begin{aligned} \delta_{c,k} &= -\frac{1}{p} \sum_{\ell=0}^{d-1} \alpha_{k\ell} \text{Ord}_c U^{\sigma_\ell}, & \gamma_{c,\ell} &= \prod_{\mathbf{a} \in \mathcal{O}_{\sigma_\ell \sigma_c}} \gamma_{\mathbf{a}}^m, & \vartheta_{c,k} &= \sum_{\ell=0}^{d-1} \alpha_{k\ell} \log |\gamma_{c,\ell}|, \\ \kappa &= \max_k \sum_{\ell=0}^{d-1} |\alpha_{k\ell}|, & \Theta &= \kappa m(p+1)|H|. \end{aligned} \quad (58)$$

where $\gamma_{\mathbf{a}}$ is defined in (18).

Remark 7.1 It is easy to see that $\delta_{c,0} = 0$ and at least one of the numbers $\delta_{c,1}, \delta_{c,2}, \dots, \delta_{c,d-1}$ is non-zero. Indeed, we have

$$\begin{pmatrix} \text{Ord}_c U^{\sigma_0} \\ \text{Ord}_c U^{\sigma_1} \\ \vdots \\ \text{Ord}_c U^{\sigma_{d-1}} \end{pmatrix} = (\log |\eta_\ell^{\sigma_k}|)_{0 \leq k, \ell \leq d-1} \begin{pmatrix} \delta_{c,0} \\ \delta_{c,1} \\ \vdots \\ \delta_{c,d-1} \end{pmatrix}. \quad (59)$$

Multiplying both sides by the d -line $(1, \dots, 1)$ on the left, we obtain $\delta_{c,0} = 0$. Further, since the column-vector on the left of (59) is non-zero, neither is the column-vector on the right.

Proposition 7.2 *Let P be an integral point on X_G having c as the nearest cusp (that is, $P \in \Omega_c$). Then for $k = 0, \dots, d-1$ we have*

$$\begin{aligned} b_k &= \delta_{c,k} \log |q_c^{-1}| + \vartheta_{c,k} \\ &+ m \sum_{\ell=0}^{d-1} \alpha_{k\ell} \left(\sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_\ell \sigma_c} \\ 0 < \tilde{a}_1 < 1/2}} \log |1 - q_c^{\tilde{a}_1} e^{2\pi i \tilde{a}_2}| + \sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_\ell \sigma_c} \\ 1/2 \leq \tilde{a}_1 < 1}} \log |1 - q_c^{1-\tilde{a}_1} e^{-2\pi i \tilde{a}_2}| \right) \\ &+ O_1(1.2\Theta|q_c|^{1/2}), \end{aligned} \quad (60)$$

where here and below we write q_c for $q_c(P)$. If, in addition, $|q_c(P)| \leq 2^{-p}$ then we also have

$$b_k = \delta_{c,k} \log |q_c^{-1}| + \vartheta_{c,k} + O_1(3.2\Theta|q_c|^{1/p}). \quad (61)$$

Further, let ν be a positive integer. Then there exist polynomials $Q_{c,k}(t) \in \mathbb{R}[t]$ of degree at most ν and satisfying $Q_{c,k}(0) = 0$ such that the following holds. Assume that

$$j(P) \notin \{1, 2, \dots, 1727\} \quad (62)$$

Then for $k = 0, \dots, d-1$ we have

$$\begin{aligned} b_k &= \delta_{c,k} \log |q_c^{-1}| + \vartheta_{c,k} \\ &+ m \sum_{\ell=0}^{d-1} \alpha_{k\ell} \left(\sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_\ell \sigma_c} \\ 0 < \tilde{a}_1 < 1/2}} |\log |1 - q_c^{\tilde{a}_1} e^{2\pi i \tilde{a}_2}|| + \sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_\ell \sigma_c} \\ 1/2 \leq \tilde{a}_1 < 1}} \log |1 - q_c^{1-\tilde{a}_1} e^{-2\pi i \tilde{a}_2}| \right) \\ &+ Q_{c,k}(q_c^{1/p}) + O_1\left(\Theta(2.2\nu/p + 3.1)|q_c|^{(\nu+1)/p}\right). \end{aligned} \quad (63)$$

(We omit the explicit formulas for the polynomials $Q_{c,k}$, which are similar to those for the real numbers $\delta_{c,k}$ and $\vartheta_{c,k}$.)

Proof As follows from Proposition 2.3, assumption (62) implies that $q_c(P) \in \mathbb{R}$. Now combining (57) and Corollary 6.5 we complete the proof. \square

In particular, we may bound b_k in terms of $q_c(P)$. Put

$$B = B(P) = \max\{|b_1|, \dots, |b_{d-1}|\} \quad (64)$$

Corollary 7.3 *In the set-up of Proposition 7.2 we have*

$$B \leq \delta_{\max} \log |q_c^{-1}| + \vartheta_{\max} + \Theta \log p. \quad (65)$$

where

$$\delta_{\max} = \delta_{\max, c} = \max_k |\delta_{c, k}|, \quad \vartheta_{\max} = \vartheta_{\max, c} = \max_k |\vartheta_{c, k}|. \quad (66)$$

If, in addition, $|q_c(P)| \leq 2^{-p}$ then we also have

$$B \leq \delta_{\max} \log |q_c^{-1}| + \vartheta_{\max} + 3.2\Theta |q_c|^{1/p} \quad (67)$$

$$\leq \delta_{\max} \log |q_c^{-1}| + \vartheta_{\max} + 1.6\Theta. \quad (68)$$

Proof For $e^{-r} < |z| < 1$ we have

$$|\log |1 - z|| \leq \max \left\{ \log 2, \log \left| \frac{1}{\log |z|} \right| + \log \frac{r}{1 + e^{-r}} \right\}. \quad (69)$$

Since $|q_c^{\tilde{a}_1}|, |q_c^{1-\tilde{a}_1}| \leq e^{-(\pi\sqrt{3})/p}$, applying (69) with $r = (\pi\sqrt{3})/5$ (recall that $p \geq 5$) gives

$$|\log |1 - q_c^{\tilde{a}_1} e^{2\pi i \tilde{a}_2}|| \leq \max \left\{ \log 2, \log \frac{p}{\pi\sqrt{3}} + 0.5 \right\} \leq \log p - 0.5,$$

and similarly for $|\log |1 - q_c^{1-\tilde{a}_1} e^{-2\pi i \tilde{a}_2}||$. Hence the sum of the logarithmic terms in the right-hand side of (60) is bounded in absolute value by $m\kappa|\mathcal{O}|(\log p - 0.5)$. This proves (65). Finally (67) is immediate from (61), and (68) is immediate from (67). \square

8 Baker's Method on $X_{\text{ns}}^+(p)$

In this section we bound the quantity $B(P)$ defined in (64) using Baker's method. We mainly follow [1], with appropriate changes.

We shall use Baker's inequality in the following form, due to Matveev [26, Corollary 2.3].

Theorem 8.1 (Matveev) *Let L be a number field of degree δ over \mathbb{Q} , embedded in \mathbb{C} . Let $\alpha_1, \dots, \alpha_n$ be non-zero elements of L , and b_1, \dots, b_n rational integers. We fix some values of logarithms $\log \alpha_1, \dots, \log \alpha_n$ and put*

$$\Lambda = b_1 \log \alpha_1 + \dots + b_n \log \alpha_n.$$

Further, let real numbers A_1, \dots, A_n satisfy

$$A_k \geq \max\{\delta h(\alpha_k), |\log \alpha_k|, 0.16\}, \quad (70)$$

where $h(\cdot)$ is the absolute logarithmic height. Finally, put

$$\mathcal{U} = A_1 \cdots A_n, \quad C(n) = 40000 \cdot 30^n n^{5.5}.$$

Then either $\Lambda = 0$ or

$$|\Lambda| > e^{-C(n)\delta^2 \mathcal{U}(1+\log \delta)(1+\log B)}. \quad (71)$$

It will be more convenient for us to use the following consequence. By the principal values of $\log z$ and $\arg z$ we mean those satisfying

$$-\pi < \operatorname{Im} \log z = \arg z \leq \pi.$$

Corollary 8.2 *In the set-up of Theorem 8.1 take the principal values of all logarithms and assume that*

$$A_k \geq \delta h(\alpha_k) + \pi \quad (k = 1, \dots, n).$$

Then we have either $\alpha_1^{b_1} \cdots \alpha_n^{b_n} = 1$ or

$$|\log(\alpha_1^{b_1} \cdots \alpha_n^{b_n})| \geq e^{-\pi C(n+1)\delta^2 \mathfrak{U}(1+\log \delta)(1+\log n+\log B)}, \quad (72)$$

again with the principal choice of the logarithm.

Proof Notice first of all that $\log |\alpha_k| \leq \delta h(\alpha_k)$ and, since we have principal values of the logarithms,

$$|\log \alpha_k| \leq \delta h(\alpha_k) + \pi.$$

Hence (70) is satisfied.

Further, there exists $b \in \mathbb{Z}$ such that

$$\log(\alpha_1^{b_1} \cdots \alpha_n^{b_n}) = \Lambda - b\pi i.$$

We may assume that $|\arg(\alpha_1^{b_1} \cdots \alpha_n^{b_n})| < \pi/2$ (otherwise there is nothing to prove), and we have $|\arg \alpha_k| \leq \pi$ by the assumption. It follows that $|b| \leq nB + 1/2$, and by integrality that $|b| \leq nB$. Now put $\alpha_{n+1} = -1$, $\log \alpha_{n+1} = \pi i$, $b_{n+1} = -b$ and $A_{n+1} = \pi$ and apply Theorem 8.1 to the logarithmic form

$$\Lambda' = \Lambda - b\pi i = b_1 \log \alpha_1 + \cdots + b_{n+1} \log \alpha_{n+1}.$$

We must replace $C(n)$ by $C(n+1)$, \mathfrak{U} by $\pi \mathfrak{U}$ and B by nB . We obtain

$$|\Lambda'| \geq e^{-\pi C(n+1)d^2 \mathfrak{U}(1+\log d)(1+\log n+\log B)},$$

as wanted. □

Now we resume the set-up of Section 7 and will use Corollary 8.2 to bound B from (64).

Proposition 8.3 *In the set-up of Proposition 7.2 assume that*

$$d \geq 3$$

(and in particular $p \geq 7$). Define

$$\begin{aligned} \mathfrak{U}_1 &= 10^8 \delta_{\max} 9^d d^6 p^{4d+2} h(\eta_1) \cdots h(\eta_{d-1}), \\ \mathfrak{U}_2 &= \mathfrak{U}_1 + \vartheta_{\max} + 4\kappa p^3, \\ B_0 &= 2\mathfrak{U}_1 \log \mathfrak{U}_1 + 2\mathfrak{U}_2, \end{aligned}$$

Then for $B = B(P) = \max\{|b_0|, \dots, |b_{d-1}|\}$ we have $B \leq B_0$.

Remark 8.4 By the famous result of Schinzel [28, 18] we have

$$h(\eta_k) \geq \frac{1}{2} \log \frac{1 + \sqrt{5}}{2} \geq 0.24 \quad (k = 1, \dots, d-1). \quad (73)$$

Since $p \geq 7$ this implies that

$$\mathfrak{U}_1 \geq 10^8 \delta_{\max} 9^d d^6 p^{3d+3}. \quad (74)$$

Proof We define the function $W \in K(X_G)$ as follows:

$$W = \begin{cases} U^{\text{Ord}_c U^\sigma} (U^\sigma)^{-\text{Ord}_c U}, & \text{Ord}_c U \neq 0, \\ U, & \text{Ord}_c U = 0 \end{cases}$$

Then $\text{Ord}_c W = 0$ and W is not a constant function by Proposition 6.9. We have

$$W(c) = \begin{cases} \gamma_{c, \mathcal{O}}^{\text{Ord}_c U^\sigma} \gamma_{c, \mathcal{O}^\sigma}^{-\text{Ord}_c U}, & \text{Ord}_c U \neq 0, \\ \gamma_{c, \mathcal{O}}, & \text{Ord}_c U = 0 \end{cases}$$

where $\gamma_{c, \mathcal{O}}$ is defined in (45). Using (46) and Proposition 6.6 we may estimate the height of $W(c)$:

$$h(W(c)) \leq \frac{\log 2}{3} mp(p+1) |H|^2. \quad (75)$$

We may assume that $|q_c(P)| \leq 1/2^p$: otherwise (65) and (74) imply that

$$B \leq 2\delta_{\max} + \vartheta_{\max} + \Theta \log p \leq \mathfrak{U}_2 \leq B_0.$$

The rest of the proof splits into two cases, treated quite differently.

Case 1: $W(P) \neq W(c)$ This is the principal case, which requires use of Baker's inequality. We have

$$1 \neq \frac{W(P)}{W(c)} = \alpha_0 \alpha_1^{b_1} \cdots \alpha_{d-1}^{b_{d-1}},$$

where

$$\alpha_0 = \begin{cases} W(C)^{-1} \eta_0^{m \text{Ord}_c U^\sigma} (\eta_0^\sigma)^{-m \text{Ord}_c U}, & \text{Ord}_c U \neq 0, \\ W(C)^{-1} \eta_0^m, & \text{Ord}_c U = 0, \end{cases}$$

$$\alpha_k = \begin{cases} \eta_k^{\text{Ord}_c U^\sigma} (\eta_k^\sigma)^{-\text{Ord}_c U}, & \text{Ord}_c U \neq 0, \\ \eta_k, & \text{Ord}_c U = 0, \end{cases} \quad (k = 1, \dots, d-1).$$

We shall apply Corollary 8.2 with $L = \mathbb{Q}(\zeta_p + \bar{\zeta}_p)$ and $\delta = (p-1)/2$. Using (55), (75) and Proposition 6.6, we obtain the estimates

$$\delta h(\alpha_0) + \pi \leq \frac{\log 2}{3} mp(p+1) \delta |H|^2 + \frac{\log 2}{6} m^2 p(p+1) \delta |H|^2 + \pi \leq 0.4p^5.$$

(recall that $|H| \leq (p-1)/3$, $p \geq 7$ and $m \leq 6$). Further, using Proposition 6.6 and (73), we obtain

$$\delta h(\alpha_k) + \pi \leq \frac{1}{6} mp(p+1) \delta |H| h(\eta_k) + \pi \leq 0.3p^4 h(\eta_k) \quad (k = 1, \dots, d-1)$$

Applying Corollary 8.2 with $n = d$ and $\mathfrak{U} = A_0 A_1 \cdots A_{d-1}$, where $A_0 = 0.4p^5$ and $A_k = 0.3p^4 h(\eta_k)$ for $k = 1, \dots, d-1$, we obtain

$$\left| \log \frac{W(P)}{W(c)} \right| = \left| \log(\alpha_0 \alpha_1^{b_1} \cdots \alpha_{d-1}^{b_{d-1}}) \right| \geq e^{-\mathfrak{U}_0(1+\log d+\log B)}, \quad (76)$$

$$\mathfrak{U}_0 = 1.6 \cdot 10^6 \cdot 9^d (d+1)^{5.5} (1+\log(d+1)) p^{4d+1} h(\eta_1) \cdots h(\eta_{d-1}).$$

On the other hand, (49) together with Proposition 6.6 implies that

$$\left| \log \frac{W(P)}{W(c)} \right| \leq 0.6 m^2 p(p+1)^2 |H|^2 |q_c(P)|^{1/p} \leq 2.4p^5 |q_c(P)|^{1/p},$$

which, together with (76) gives

$$\log |q_c(P)^{-1}| \leq p\mathfrak{U}_0(\log B + \log d + 1) + 6p \log p.$$

Combining this with (68), we obtain

$$\begin{aligned} B &\leq p\delta_{\max}\mathfrak{U}_0 \log B + p\delta_{\max}\mathfrak{U}_0(\log d + 1) + 6\delta_{\max}p \log p + \vartheta_{\max} + 1.6\Theta \\ &\leq \mathfrak{U}_1 \log B + \mathfrak{U}_2. \end{aligned}$$

Now Lemma 2.3.3 from [7] implies that $B \leq 2\mathfrak{U}_1 \log \mathfrak{U}_1 + 2\mathfrak{U}_2$, as wanted.

Case 2: $W(P) = W(c)$ In this case Baker's inequality does not apply. Instead, we invoke an elementary argument using power series expansion of W .

For a moment we forget that we fixed P and consider P as a varying point in Ω_c . Propositions 6.4 and 6.6 imply that for $k = 1, 2, \dots$ there exist algebraic numbers $\theta_k \in \mathbb{Q}(\zeta_p)$ such that for any absolute value v of $\mathbb{Q}(\zeta_p)$ we have

$$|\theta_k|_v \leq \begin{cases} |k|_v^{-1}, & v \mid p < \infty, \\ \frac{1}{3}m^2p(p+1)^2|H|^2(k/p+1), & v \mid \infty \end{cases} \quad (k = 1, 2, \dots) \quad (77)$$

and the following holds. Let ν be a non-negative integer. Then for $P \in \Omega_c$ such that $|q_c(P)| < 1/2^p$ we have, with a suitable choice of logarithms,

$$\log \frac{W(P)}{W(c)} = \sum_{k=1}^{\nu} \theta_k q_c(P)^{k/p} + O_1 \left(\frac{1}{6}m^2p(p+1)^2|H|^2(2.2\nu/p + 5.1) |q_c(P)|^{(\nu+1)/p} \right).$$

Now specify ν to be the smallest k such that $\theta_k \neq 0$. (Since the function W is non-constant such k always exist.) With this choice of ν the relation above would look like

$$\log \frac{W(P)}{W(c)} = \theta_{\nu} q_c(P)^{\nu/p} + O_1 \left(\frac{1}{6}m^2p(p+1)^2|H|^2(2.2\nu/p + 5.1) |q_c(P)|^{(\nu+1)/p} \right). \quad (78)$$

Also, (77) with $k = \nu$ implies that

$$\mathfrak{h}(\theta_{\nu}) \leq \log \left(\frac{1}{3}m^2p(p+1)^2|H|^2(\nu/p+1) \right) + \log \nu,$$

Since $\theta_{\nu} \neq 0$ and $\theta_{\nu} \in \mathbb{Q}(\zeta_p)$, this implies that

$$|\theta_{\nu}| \geq e^{-(p-1)\mathfrak{h}(\theta_{\nu})} \geq \left(\frac{1}{3}m^2p(p+1)^2|H|^2(\nu/p+1)\nu \right)^{-(p-1)}. \quad (79)$$

We now return to the initial set-up of the proof: P is an integral point belonging to Ω_c and satisfying $W(P) = W(c)$. Then the logarithm on the left of (78) is either 0 or at least 2π in absolute value. We consider these cases separately.

Sub-case 2.1: the logarithm on the left of (78) is 0. In this case we have

$$\theta_{\nu} q_c(P)^{\nu/p} = O_1 \left(\frac{1}{6}m^2p(p+1)^2|H|^2(2.2\nu/p + 5.1) |q_c(P)|^{(\nu+1)/p} \right).$$

Together with (79) this implies

$$|q_c(P)^{-1}| \leq \left(\frac{m^2p(p+1)^2|H|^2(2.2\nu/p + 5.1)}{6\theta_{\nu}} \right)^p \leq \left(\frac{1}{2}m^2p(p+1)^2|H|^2(\nu/p+1)\nu \right)^{p^2} \quad (80)$$

To complete the proof we need to bound ν . We claim the following.

Claim *There exists $k \leq \frac{1}{288}m^2p^2(p-1)(p+1)^2|H|^2$ such that $\theta_k \neq 0$.*

We assume the claim for now, postponing the proof until later. By the claim,

$$\nu \leq \frac{1}{288}m^2p^2(p-1)(p+1)^2|H|^2,$$

which implies that

$$|q_c(P)^{-1}| \leq \left(\frac{1}{576}m^4p^3(p+1)^4(p-1)|H|^4 \left(\frac{1}{288}m^2p^2(p-1)(p+1)^2|H|^2 + 1 \right) \right)^{p^2} \leq p^{19p^2}.$$

Together with (68) this implies that

$$B \leq 19\delta_{\max}p^2 \log p + \vartheta_{\max} + 1.6\Theta \leq \mathfrak{U}_2 \leq B_0$$

by (74).

Sub-case 2.2: the logarithm on the left of (78) is at least 2π in absolute value. In this case a bound for $|q_c(P)^{-1}|$ much sharper than (80) easily follows. We omit the details which are straightforward but tedious.

We are left with proving the Claim.

Proof of the Claim Denote by Δ the degree of W as a rational function on X_G . Then the function $W/W(c) - 1$ is of degree Δ as well. It follows that $\text{Ord}_c(W/W(c) - 1) \leq \Delta$.

Extend the additive valuation Ord_c from the field $\mathbb{C}(X_G)$ to the field of formal power series $\mathbb{C}((q_c^{1/p}))$. Then $\text{Ord}_c(q_c^{1/p}) = 1$ and $\text{Ord}_c \log(W/W(c)) = \text{Ord}_c(W/W(c) - 1) \leq \Delta$. It follows that the series in $q_c^{1/p}$ representing $\log(W/W(c))$ has a non-zero coefficient with index $k \leq \Delta$.

Proposition 6.6 implies that $\Delta \leq \frac{1}{288}m^2p^2(p-1)(p+1)^2|H|^2$. This proves the claim. \square

9 Reduction of Baker's Bound

In the previous section we bounded $B = \max\{|b_1|, \dots, |b_{d-1}|\}$ by an explicitly computable number B_0 . In practical situation B_0 can be very huge (around 10^{100} or so), so not suitable for direct enumeration of all possible vectors (b_1, \dots, b_{d-1}) . It turns out, however, that it can be drastically reduced, using the numerical Diophantine approximations technique introduced by Baker and Davenport [3] and developed in [7, 34] in the context of the Diophantine equation of Thue.

It turns out that the method of [7], suitably adapted, works in the present situation as well. As in the previous section we fix a cusp c and consider integral points $P \in \Omega_c$. We shall usually omit index c , writing as $\delta_{c,k} = \delta_k$ and $\vartheta_{c,k} = \vartheta_k$ the quantities defined in (58).

As we have seen in Remark 7.1, at least one of the numbers $\delta_1, \dots, \delta_{d-1}$ is non-zero. To simplify notation we will assume that $\delta_1 \neq 0$.

It turns out to be more practical to obtain a reduced bound for $\log |q_c(P)^{-1}|$; due to the results of Section 7 this would imply reduced bounds for the exponents b_k . In this section we will assume that

$$|q_c(P)| \leq \max\{\Theta, 2\}^{-p}, \tag{81}$$

where Θ is defined in (58).

Put

$$\delta = \frac{\delta_2}{\delta_1}, \quad \lambda = \frac{\delta_2\vartheta_1 - \delta_1\vartheta_2}{\delta_1}$$

Relation (61) implies that

$$|b_2 - \delta b_1 + \lambda| \leq 3.2(1 + |\delta|)\Theta |q_c(P)|^{1/p}, \tag{82}$$

To bound $\log |q_c(P)^{-1}|$ we proceed now as follows. We fix a real number $T \geq 2$ (in practice, we take $T = 10$). Next, using continued fraction we find a “good” rational approximation of δ ; precisely, we find a non-negative integer $r \leq TB_0$ such that

$$\|r\delta\| \leq (TB_0)^{-1}$$

where $\|\cdot\|$ is the distance to the nearest integer. Now, if $r\lambda$ is not “very close” to the nearest integer (in practice if $\|r\lambda\| \geq 2T^{-1}$) then we can bound $|q_c(P)^{-1}|$. Indeed, multiply both sides of (82) by r . Since $|b_1| \leq B_0$, the left-hand side of the resulting inequality would be

$$|rb_2 - r\delta b_1 + r\lambda| \geq \|r\lambda\| - B_0\|r\delta\| \geq \|r\lambda\| - T^{-1},$$

and the right-hand side will be bounded from above by $3.2(1 + |\delta|)\Theta TB_0 |q_c(P)|^{1/p}$. This gives the following upper bound for $|q_c(P)^{-1}|$:

$$\log |q_c(P)^{-1}| \leq p \log \frac{3.2(1 + |\delta|)\Theta TB_0}{\|r\lambda\| - T^{-1}} =: \Xi_1. \quad (83)$$

In the case when $\|r\lambda\| < 2T^{-1}$ we increase T (say, replace it by $10T$) and restart.

Substituting (83) into (61) and using (81), we obtain a new bound for b_1 :

$$|b_1| \leq |\delta_1|\Xi + |\vartheta_1| + 3.2 =: B_1.$$

Since B_1 depends logarithmically on B_0 , it is expected to be much smaller than B_0 , and in practice it is.

We then repeat the same procedure, but this time with B_1 instead of B_0 , and obtain for $\log |q_c(P)^{-1}|$ and $|b_1|$ new reduced bounds Ξ_2 and B_2 , and so on. In practice, after three-four iterations of this procedure we obtain bounds for $\log |q_c(P)^{-1}|$ and $|b_1|$ that can no longer be reduced. We call $\widehat{\Xi}$ this reduced bound for $\log |q_c(P)^{-1}|$. In practice $\widehat{\Xi}$ is of order about 10^3 .

To be precise, since we assumed (81), we must replace $\widehat{\Xi}$ by $\max\{\widehat{\Xi}, p \log \Theta, p \log 2\}$. But in all practical cases we had $\widehat{\Xi} > p \log \Theta > p \log 2$ with large margins.

10 Final enumeration

The reduced upper bound for $\log |q_c(P)^{-1}|$ obtained in the previous section allows one to bound the exponents b_1, \dots, b_{d-1} by some reasonable quantities (of magnitude 10^5 or so). Still, the number of possible vectors (b_1, \dots, b_{d-1}) is excessively large, and they cannot be fully enumerated in reasonable time.

In the similar situation in [7] it was suggested to express all the b_k in terms of one of them, say, b_1 . Then, for each possible value of b_1 one calculates the corresponding values of other b_k , and if one of these values is not integer, then the corresponding value of b_1 is impossible.

We apply the same methodology here, though in the present situation the technical aspect is much more involved. In the sequel we shall assume that $q_c(P) \in \mathbb{R}$, which, according to Proposition 2.3, is equivalent to saying that $j(P) \notin \{1, 2, \dots, 1727\}$. In Subsection 10.4 we briefly discuss how we dispose of these missing j .

Like in Section 9, we omit indice c and write $\delta_{c,k} = \delta_k$ and $\vartheta_{c,k} = \vartheta_k$, etc. Recall that these quantities, as well as the quantity Θ used below are defined in (58).

10.1 Quick enumeration

If $\log |q_c(P)^{-1}|$ is not too small then one can express b_2, \dots, b_{d-1} in terms of b_1 with high precision using relation (61), as it is done for b_2 in (82). For the reader’s convenience, we reproduce relation (61), which is our main tool in this subsection: for $k = 1, \dots, d-1$ and $|q_c(P)| \leq 1/2^p$ we have

$$b_k = \delta_k \log |q_c(P)^{-1}| + \vartheta_k + O_1(3.2\Theta |q_c(P)|^{1/p}). \quad (84)$$

Proposition 10.1 *Let Y be a real number satisfying $p \log 2 \leq Y \leq \widehat{\Xi}$. Put $\epsilon = 3.2|\delta_1|^{-1}\Theta e^{-Y/p}$. In the set-up of Proposition 7.2 assume that $\log |q_c(P)^{-1}| \geq Y$. Then*

$$Y - \epsilon \leq \ell_1 \leq \widehat{\Xi} + \epsilon, \quad \text{where } \ell_1 = \frac{b_1 - \vartheta_1}{\delta_1}. \quad (85)$$

Further, for $k = 2, \dots, d-1$ we have

$$|b_k - (\delta_k \ell_1 + \vartheta_k)| \leq \left(1 + \left|\frac{\delta_k}{\delta_1}\right|\right) \epsilon_1, \quad (86)$$

where $\epsilon_1 = 3.2\Theta e^{(\epsilon - \ell_1)/p}$.

Proof We write q instead of $q_c(P)$. Assume that $\log |q^{-1}| \geq Y$. Then $Y \leq \log |q^{-1}| \leq \widehat{\Xi}$ and $|q|^{1/p} \leq e^{-Y/p}$. We obtain from (84) with $k = 1$ that $|\ell_1 - \log |q^{-1}|| \leq \epsilon$, which implies, in particular, (85). Furthermore, we have $\log |q^{-1}| \geq \ell_1 - \epsilon$, which gives $3.2|\Theta||q|^{1/p} \leq \epsilon_1$. Again using (84) with $k = 1$, we obtain $|\ell_1 - \log |q^{-1}|| \leq |\delta^{-1}| \epsilon_1$. All this combined with relations (84) for $k = 2, \dots, d-1$ gives (86). \square

In practice we initially set $Y = p \log(50|\delta_1|^{-1}\Theta)$. We list integers b_1 satisfying (85) in the descending order of ℓ_1 , and for each b_1 we verify whether each of the $d-2$ intervals

$$\left[\delta_k \ell_1 + \vartheta_k - \left(1 + \left|\frac{\delta_k}{\delta_1}\right|\right) \epsilon_1, \delta_k \ell_1 + \vartheta_k + \left(1 + \left|\frac{\delta_k}{\delta_1}\right|\right) \epsilon_1 \right] \quad (2 \leq k \leq d-1), \quad (87)$$

contains an integer. If at least one of these intervals does not contain an integer we pass to the next b_1 in the list. Otherwise, we re-set $Y = \ell_1 + \epsilon$ and terminate the algorithm. At the output, we obtain a new upper bound Y for $\log |q_c(P)^{-1}|$.

Remark 10.2 The choice of b_1 as the “independent variable” is quite arbitrary; any b_k with $\delta_k \neq 0$ would do. We believe that the optimal choice is the one with the smallest (in absolute value) non-zero δ_k , because it minimizes the range of possible values for b_k .

10.2 Slow enumeration: the overview

When $\log |q_c(P)^{-1}| \leq Y$, simple relations (84) is no longer sufficient to express b_2, \dots, b_{d-1} in terms of b_1 , and one has to use more complicated relations like (63). For the reader's convenience, we reproduce (63) below. Let ν be a positive integer and let $Q_k(t)$ be the polynomials $Q_{c,k}(t)$ (depending on ν) defined in Proposition 7.2. For $k = 1, \dots, d-1$ define the functions of the real variable t by

$$f_k(t) = -p\delta_k \log |t| + \vartheta_c + Q_\nu(t) + m \sum_{\ell=0}^{d-1} \alpha_{k\ell} \left(\sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_\ell} \sigma_c \\ 0 < \bar{a}_1 < 1/2}} \log |1 - t^{p\bar{a}_1} e^{2\pi i \bar{a}_2}| + \sum_{\substack{\mathbf{a} \in \mathcal{O}_{\sigma_\ell} \sigma_c \\ 1/2 \leq \bar{a}_1 < 1}} \log |1 - t^{p-p\bar{a}_1} e^{-2\pi i \bar{a}_2}| \right).$$

Then, setting $t = q_c(P)^{1/p}$, we have, for $k = 1, \dots, d-1$, the following:

$$b_k = f_k(t) + O_1(\Theta(2.2\nu/p + 3.1)|t|^{\nu+1}), \quad (88)$$

where Θ is defined in (58). We have either $q_c(P) \geq e^{-2\pi}$ or $q_c(P) \leq -e^{-\pi\sqrt{3}}$. Since $\log |q_c(P)| \leq Y$, we obtain

$$t \in [-e^{-\pi\sqrt{3}/p}, -e^{-Y/p}] \cup [e^{-Y/p}, e^{-2\pi/p}]. \quad (89)$$

The principal steps of the final enumeration procedure can be described as follows.

1. Split domain (89) into intervals of monotonicity of the function f_1 .
2. Let I be one of the intervals found on step 1 and $J = f_1(I)$. Fix $b_1 \in J$ and compute $t \in I$ such that $f_1(t) = b_1$. Since f_1 is monotonic on I , only one such t may exist. (Since equality in (88) is approximate, one should not miss the possible b_1 outside the interval J , but close to it; see more on this Subsection 10.3.)
3. The real number $f_k(t)$ must then be “very close” to the integer b_k , for $k = 2, \dots, d-1$. If this fails for at least one k , we discard the corresponding b_1 .
4. If each of $f_k(t)$ is close to an integer, then we compute $j(t^p)$ (for this purpose, we might need to know t with higher precision than on step 3, see Subsection 10.3). If it is approximately equal to an integer j , then we verify whether j gives rise to an integral point on $X_{\text{ns}}^+(p)$.
5. Steps 2–4 should be repeated for all $b_1 \in J$.
6. Step 5 must be repeated for every interval of monotonicity of f_1 .

In Subsection 10.3 we add some computational details on these steps.

10.3 Slow enumeration: computational remarks

Notice first of all that one should take care about the computational errors arising from the very fact that our numerical data is given approximately. This also concerns the reduction and the quick enumeration steps. This is a standard problem in the numerical analysis, and we do not speak on it here, but we had to take care of it in our software implementations.

The monotonicity intervals To determine the monotonicity intervals of f_1 , one should find the zeros of its derivative. This derivative is a rational function, and its zeros can be found using any of the available methods for numerical solution of polynomial equation.

We used Brent’s method, implemented in PARI, which efficiently combines several known methods of numerical resolution of equation. In most of the cases f_1 was monotonic already on each of the two intervals forming domain (89), but in a few cases we had to split them into smaller intervals.

Resolving the equation $f_1(t) = b_1$ and computing $f_k(t)$ Here we give some clarifications on the steps 2 and 3 of the slow enumeration procedure. Thus, we assume that t belongs to some interval $I = [\alpha, \beta]$ and that f_1 is monotonic on I . Let

$$\epsilon = \Theta(2.2\nu/p + 3.1) e^{-(\nu+1)\pi\sqrt{3}/p} \quad (90)$$

be an upper bound for the error term in (88), and let $b_1 \in [\alpha - \epsilon, \beta + \epsilon]$. Using Brent’s method, we compute the solutions $t \in I$ of $f_1(t) = b_1 \pm \epsilon$; call them τ^+ and τ^- . In the (rare) case when $b_1 - \epsilon \notin I$ we replace $b_1 - \epsilon$ by α , and similarly for $b_1 + \epsilon$. Now b_k must be between $f_k(\tau^-)$ and $f_k(\tau^+)$ (except the very few cases when f'_k vanishes between these points, and one has to be slightly more careful). For overwhelming majority of choices of b_1 , at least one of the $d-2$ intervals

$$[\min\{f_k(\tau^-), f_k(\tau^+)\} - \epsilon, \max\{f_k(\tau^-), f_k(\tau^+)\} + \epsilon], \quad k = 2, \dots, d-1 \quad (91)$$

does not contain an integer, and the corresponding b_1 can be discarded. In the few cases when this fails, one may refine intervals (91), in one of the following ways.

- Replace ϵ by

$$\epsilon_1 = \Theta(2.2\nu/p + 3.1) (\min\{\tau^-, \tau^+\})^{-(\nu+1)}.$$

Then τ^- and τ^+ will be replaced by certain τ_1^- and τ_1^+ , which lie much closer to each other than τ^- and τ^+ , and intervals (91) will be modified accordingly.

- Increase ν and re-define functions f_1, \dots, f_{d-1} accordingly.

Acting like this, we managed to exclude almost all the false positives.

Computing j and verifying whether it gives rise to an integral point If everything above fails to discard b_1 , then probably this b_1 indeed corresponds to an integral point. To verify this, we compute $j = j(t^p)$. For this we need knowing t with much higher precision than in the previous steps of the algorithm. Therefore we have to increase ν , re-define f_1 and re-calculate t with higher precision, then find $j(t^p)$ and see whether it lies close to an integer within the computational error. In all cases when it did, j was a rational CM j -invariant, that is, one of the 13 numbers from the bottom line of Table 1 on page 2.

Selection of ν Selecting the parameter ν correctly is quite important for optimizing the calculations. When ν is chosen too small, then precision of (88) would be insufficient; but choosing ν too high leads to too complicated expressions for $f_k(t)$ and makes the Brent’s method too slow. Our experimentation shows that the nearly optimal value for ν is the one making the error term in (88) bounded by 10^{-10} ; that is, the quantity ϵ defined in (90) should be about 10^{-10} .

Remark 10.3 The “slow enumeration” step is the bottleneck of the method, it accounts for more than 90% of the computational time. There are several possible way to accelerate this step.

- Refining the error term in (84) and (88). In particular, refining the error term in (84) would lead to more efficient “quick reduction step”, and, as a result, would reduce the domain (89) for t in the slow reduction.
- Using different expressions for the functions f_k , with fewer logarithmic terms; this can be achieved by replacing the logarithmic terms involving higher powers of t by their finite Taylor expansions, and merging these expansions with the polynomial $Q_k(t)$.
- Splitting the domain (89) into smaller parts, and using on each a more adapted expression for this domain; for instances, for smaller t we need smaller ν and fewer logarithmic terms.

We are experimenting with these approaches and will report on our experiments in subsequent publications.

10.4 The Case $j(P) \in \{1, 2, \dots, 1727\}$

Recall that to an elliptic curve E/\mathbb{Q} and a prime number p we associate a Galois representation $\rho_{E,p} : \text{Gal}_{\mathbb{Q}} \rightarrow \text{GL}(E[p]) \cong \text{GL}_2(\mathbb{F}_p)$, which is defined by the natural action of the absolute Galois group $G_{\mathbb{Q}}$ on the torsion group $E[p]$. Points in $X_{\text{ns}}(p)(\mathbb{Q})$ correspond to the elliptic curves E/\mathbb{Q} such that the image of $\rho_{E,p}$ is contained in the normalizer of a non-split Cartan subgroup of $\text{GL}_2(\mathbb{F}_p)$.

It is known that, if this latter property holds for some elliptic curve E/\mathbb{Q} with $j(E) \neq 0, 1728$, then it holds for any quadratic twist of E , that is, for any other elliptic curve E' with $j(E') = j(E)$. Indeed, E' is isomorphic to E over some field K of degree at most 2. Denote by χ_K is the character of $G_{\mathbb{Q}}$ corresponding to K . Then $\rho_{E',p} = \rho_{E,p} \chi_K$. Hence if the image of $\rho_{E,p}$ is contained in the normalizer of a non-split Cartan subgroup, then so is the image of $\rho_{E',p}$.

Hence, if we fix $j \in \mathbb{Q}$, distinct from 0 and 1728, then, to verify whether $X_{\text{ns}}(p)$ has a rational point P with $j(P) = j$, it suffices to verify for at least one curve E/\mathbb{Q} with $j(E) = j$ whether the image of $\rho_{E,p}$ is contained in the normalizer of a non-split Cartan subgroup. This can be easily accomplished with the **SAGE** package [37], functions **EllipticCurve** and **image_type**. Using it, we found that $X_{\text{ns}}(p)(\mathbb{Q})$ has no points with j -invariants from the set $\{1, \dots, 1727\}$ for all p we considered.

Acknowledgments Yuri Bilu was supported by the *Agence National de la Recherche* project “Hamot” (ANR 2010 BLAN-0115-01) and by the ALGANT scholarship program. We thank Julia Baoulina, Andreas Enge, Pierre Parent and Sha Min for useful discussions and suggestions.

Our algorithms are implemented using the computer algebra systems **PARI/GP** [36] and **SAGE** [37].

References

- [1] A. BAJOLET, M. SHA, Bounding j -invariant of integral points on $X_{\text{ns}}^+(p)$, *Proc. Amer. Math. Soc.*, to appear.
- [2] A. BAKER, Linear forms in the logarithms of algebraic numbers, I–IV, *Mathematika* **13** (1966), 204–216; **14** (1967), 102–107; **14** (1967), 220–228; **15** (1968), 204–216.
- [3] A. BAKER, H. DAVENPORT, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford (2)* **20** (1969), 129–137.
- [4] B. BARAN, A modular curve of level 9 and the class number one problem, *J. Number Th.* **129** (2009), 715–728.
- [5] B. BARAN, Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem, *J. Number Th.* **130** (2010), 2753–2772.
- [6] YU. BILU, Baker’s method and modular curves, *A Panorama of Number Theory or The View from Baker’s Garden* (edited by G. Wüstholz), 73–88, Cambridge University Press, 2002.
- [7] YU. BILU, G. HANROT, Solving Thue equations of high degree, *J. Number Th.* **60** (1996), 373–392.
- [8] YU. BILU, G. HANROT, Solving superelliptic Diophantine equations by Baker’s method, *Compositio Math.* **112** (1998), 273–312.
- [9] YU. BILU, G. HANROT, Thue equations with composite fields, *Acta Arith.* **88** (1999), 311–326.
- [10] YU. BILU, G. HANROT, P. VOUTIER (with an appendix by M. MIGNOTTE), Existence of primitive divisors of Lucas and Lehmer numbers, *J. reine angew. Math.* **539** (2001), 75–122.
- [11] YU. BILU, M. ILLENGO, Effective Siegel’s Theorem for Modular Curves, *Bull. London Math. Soc.*, **43** (2011), 673–688.
- [12] YU. BILU, P. PARENT, Runge’s Method and Modular Curves, *Int. Math. Research Notes* **2011**, 1997–2027.
- [13] YU. BILU, P. PARENT, Serre’s Uniformity Problem in the Split Cartan Case, *Ann. Math. (2)* **173** (2011), 569–584.
- [14] YU. BILU, P. PARENT, M. REBOLLEDO, Rational points on $X_0^+(p^r)$, *Ann. Inst. Fourier*, to appear.
- [15] I. CHEN, C. CUMMINS, Elliptic curves with non-split mod 11 representations, *Math. Comp.* **73** (246) (2004), 869–880.
- [16] G. HANROT, Solving Thue equations without the full unit group, *Math. Comp.* **69** (2000), 395–405.
- [17] K. HEEGNER, Diophantische Analysis und Modulfunktionen, *Math. Z.* **59** (1952) 227–253.
- [18] G. HÖHN, N.-P. SKORUPPA, Un résultat de Schinzel, *J. Th. Nombres Bordeaux* **5** (1993), 185.
- [19] M.A. KENKU, A note on the integral points of a modular curve of level 7, *Mathematika* **32** (1985), 44–48.
- [20] J. K. KOO, D. H. SHIN, On some arithmetic properties of Siegel functions, *Math. Z.* **264** (2010), 137–177.
- [21] D. S. KUBERT, S. LANG, *Modular units*, Grundlehren Math. Wiss. 244, Springer, New York-Berlin, 1981.
- [22] S. LANG, *Elliptic Functions*, Addison-Wesley, 1973.
- [23] S. LANG, *Introduction to Modular Forms*, Springer, 1978.
- [24] R. LIDL, H. NIEDERREITER, *Finite Fields*, second edition, Cambridge Univ. Press, Cambridge, 1997.
- [25] B. MAZUR, Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.* **44** (1978), 129–162.
- [26] E. M. MATVEEV, An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers II (Russian), *Izv. RAN, Ser. Mat.* **64** (2000), 125–180; (=Izv. Math. **64** (2000), 1217–1269.)
- [27] A. PETHŐ, R. SCHULENBERG, Effektives Lösen von Thue Gleichungen, *Publ. Math. Debrecen* **34** (1987), 189–196.
- [28] A. SCHINZEL, Addendum to the paper: “On the product of the conjugates outside the unit circle of an algebraic number”, *Acta Arith.* **26** (1974/75), 329–331.
- [29] R. SCHOOF, N. TZANAKIS, Integral points of a modular curve of level 11, *Acta Arith.* **152** (2012), 39–49.
- [30] J.-P. SERRE, *Lectures on the Mordell-Weil Theorem*, 3rd edition, Asp. Math. E15, Vieweg & Sohn, Braunschweig/Wiesbaden, 1997.
- [31] M. SHA, Bounding j -invariant of integral points on modular curves, submitted.
- [32] M. SHA, *Explicit Bounds for Integral Points on Modular Curves*, Ph.D. thesis, in preparation.
- [33] C.L. SIEGEL, Zum Beweise des Starkschen Satzes, *Invent. Math.* **5** (1968), 180–191.
- [34] N. TZANAKIS, B. M. M. DE WEGER, On the practical solution of the Thue equation, *J. Number Theory* **31** (1989), 99–132.
- [35] K. YU, p -adic logarithmic forms and group varieties III, *Forum Math.* **19** (2007), 187–280.
- [36] <http://pari.math.u-bordeaux.fr/>
- [37] <http://www.sagemath.org/>